# 8190 IP Speaker-Clock - User Guide

The 8190 IP Speaker – Clock is a SIP-compliant, multicast-capable IP speaker designed for any application that requires crisp clear voice paging, loud ringing, and alert/notification with a high visibility clock. The 8190 can be integrated with any communication server
(hosted or enterprise) that supports 3rd-party SIP endpoints or multicast.

The 8190 uses a multi-speaker line array for improved sound distribution. Controlled dispersion in the vertical axis reduces reflections from floor and ceiling and provides more consistent direct sound levels for listeners at different distances from the speaker.

Like other Algo IP speakers, the 8190 has a microphone for monitoring and adapting to ambient noise levels. This means voice paging and bell tones are always heard but never too loud. The microphone can also be enabled for hands-free talkback. Additionally, the 8190 has an integrated digital clock, integrated call button, and entrance security door control capability.


**Warning**

This guide provides important safety information that should be read thoroughly before permanently installing the speaker. It should be noted that this device:

- Is intended for dry indoor locations only.
- Uses a CAT5 or CAT6 connection wiring  to an IEEE 802.3at PoE+ or 802.3af compliant network PoE switch that must not leave the building perimeter without adequate lightning protection.

For more details, please see **Product Warning** below.

**Disclaimer**

The information contained in this document is believed to be accurate in all respects but is not warranted by Algo. The information is subject to change without notice and should not be construed in any way as a commitment by Algo or any of its affiliates or subsidiaries. Algo and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. Algo assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware.



For additional information or technical assistance in North America, please contact Algo's support team:
1-604-454-3792
support@algosolutions.com

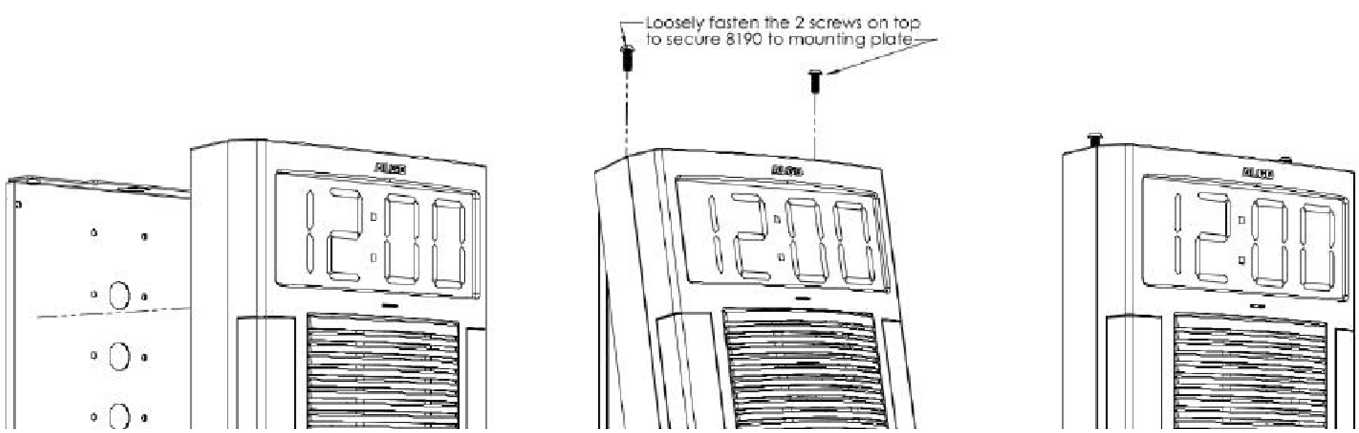
# Setup and Installation

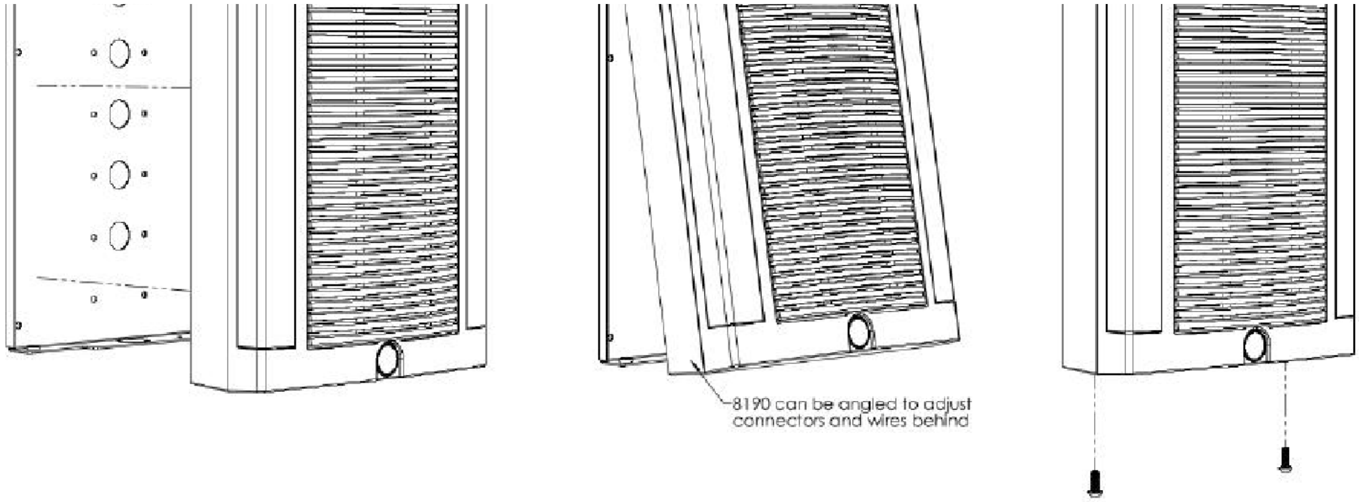
**What's Included**

- 8190 IP Speaker – Clock
- Wall-mount bracket
- Algo screwdriver

## Mounting

Securely mount the supplied wall bracket. Once the wall bracket is secure, slide the 8190 onto the bracket. Secure the 8190 to the wall bracket with the provided four screws.






## Wiring

The 8190 has an RJ45 jack for network connection. A cable run from the switch can be terminated in one of two ways: 1) to a modular jack with connection by patch cord or 2) terminated with an RJ45 plug.

PoE (Power over Ethernet) must be 48V 350 mA IEEE 802.3at PoE+ or 802.3af compliant whether provided by the network switch or injector. If you don't have a PoE switch, you'll need a PoE or PoE+ injector installed between the 8190 and the network switch. The PoE injector will supply 48 Vdc to the 8190. Most PoE injectors are capable of providing more power than the 8190 requires (12.95 W). Ensure that the PoE injector is fully compliant to the IEEE 802.3at PoE+ or 802.3af standard.

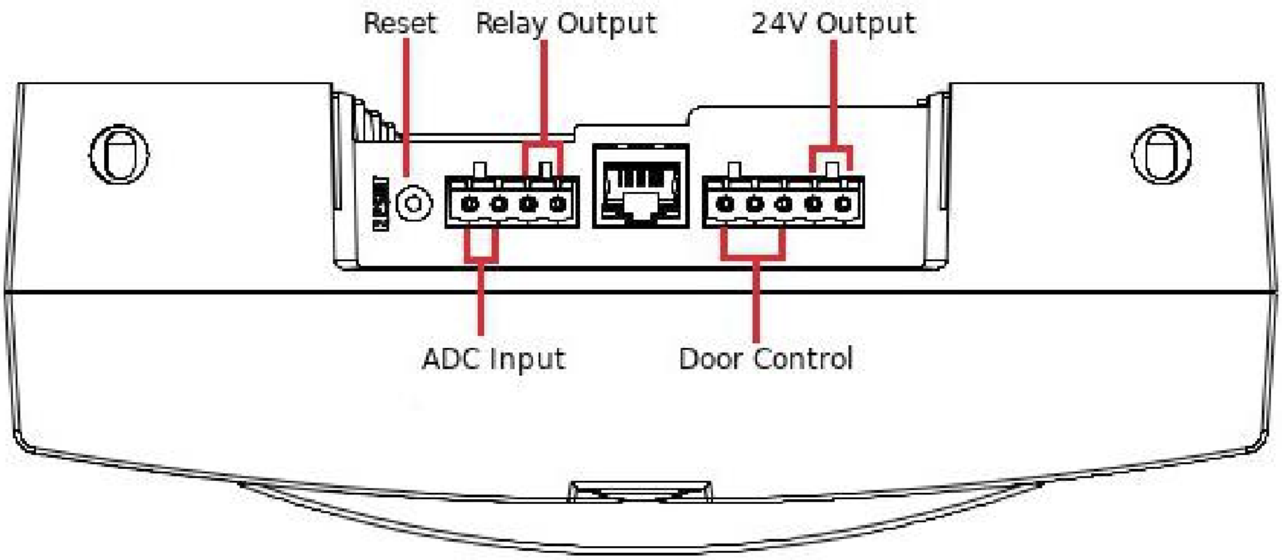
There are two lights on the Ethernet jack:

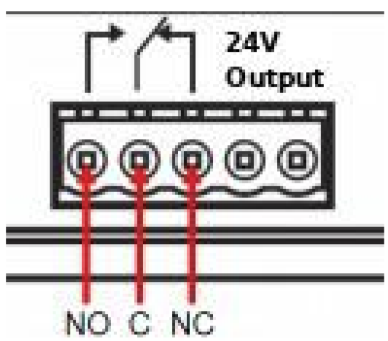
- Green light - On when Ethernet is working. Flickers off to indicate activity on the port.
- Amber light - Off when successful 100 Mbps link is established. Typically only on briefly at power up.

Under normal conditions, the amber light will turn on immediately after the Ethernet cable is first connected. This indicates that PoE power has been successfully applied. Once the device connects to the network, the amber light will turn off and the green light will turn on. The green light will flicker to indicate there is traffic on the network.

## Inputs/Outputs

The 8190 has an ADC input, relay output, 24V output, and a door control relay on the bottom of the device.




| | |
|---|---|
| Terminal Block ADC Input | By default, these terminals are inactive. Connection options are a normally closed switch, normally open switch, 1202 Call Button, 1203 Call Switch, or EOL resistor termination. |
| Terminal Block Relay Out | By default these terminals provide a contact closure when the 8190 is active. |
| Door Control | The door control provides both normally open (NO), common (C), and normally closed (NC) relay contacts.   |

## Accessing the Web Interface

Configuration of the 8190 can be completed via the device web interface by entering the IP address of the device in a web browser. The web interface does not require additional purchase. All settings, integrations, and file uploads can be accessed via the web interface. See the configuration chapters below for more details. To access the web interface:

1. Connect the 8190 IP Speaker – Clock to an IEEE 802.3at PoE+ or IEEE 802.3af PoE

compliant network switch. The blue light will remain on until boot-up is completed – about 45 seconds.

2. After the blue LED turns off and you hear a tone, press the reset switch (RST) button on the back of the unit to hear the IP address over the speaker. Press the RST button again to stop playing the IP address. The device's IP address can also be found by using an IP scanner tool such as Angry IP Scanner which is free and open-source.

   If the 8190 is not able to obtain an IP address from the DHCP server, the 8190 will default to the static IP address 192.168.1.111

3. Type the device IP address into a web browser to access the web interface and configure the device. Note that these devices may also or alternatively be configured using centralized provisioning or the Algo Device Management Platform (ADMP).
4. Login using the default password: *algo.*

## Example Testing Configuration

1. After logging into the 8190 web interface, navigate to **Basic Settings** → **SIP** and enter the IP address or the domain name for the SIP server (provided by your IT team or hosted provider) into **SIP Domain (Proxy Server)**.
2. Enter the Page and/or Ring credentials **Extension**, **Authentication ID**, and **Authentication Password** (provided by your IT team or hosted provider). If you are not using an extension, leave the fields blank. Note that some SIP servers may say Username instead of Authentication ID.
3. Verify the extension is properly registered with the SIP server in the Status tab. Ensure the SIP registration says “Successful”.
4. Test the speaker by dialing the registered SIP extension from an IP phone connected to your network.

## Reset

A recessed reset button (RST) on the back can be used to reset the 8190 speaker during power-up. A reset will set all configuration options to factory default including the password.

To reset:

1. Reboot or power cycle the 8190.
2. Wait until the blue LED flashes and then press and hold the reset button until the blue LED begins a double flash pattern.
3. Release the reset button and allow the unit to complete its boot process. Do not press the reset button until the blue LED begins flashing.

Once booting has completed, pressing the reset button will cause the speaker to announce its IP address over the speaker.

## Check Device Status

The web interface has a Status page which, by default, is available with and without a login. The Status page can be made exclusive to logged-in users via **Advanced Settings** → **Admin** → **General** → **Show Status Section on Status Page when Logged Out.**

The Status page contains information such as:

| | |
|---|---|
| • Device Name<br>• SIP Registration<br>• Call Status<br>• Proxy Status<br>• Provisioning Status<br>• MAC<br>• IPv4<br>• IPv6 | • Date/Time<br>• Multicast Mode<br>• Volume<br>• Relay Input Status<br>• InformaCast License<br>• ADMP Cloud Monitoring |

## Register Your Product

You may register your product at https://www.algosolutions.com/product-registration/ to ensure access to the latest upgrades for your device and to receive important service notices.

## Security

Algo devices use TLS for provisioning and SIP signaling to mitigate cyberattacks by those trying to intercept, replicate, or alter Algo products. Algo devices also come pre-loaded with certificates from a list of trusted certificate authorities (CA) to ensure secure communication with reputable sources. Pre-installed trusted certificates are not visible to users and are separate from those in the 'certs' folder.

For further details, see Securing Algo Endpoints: TLS and Mutual Authentication.

---

# Common Configurations

The 8190 can be used in various ways to enhance paging and alerting systems. The most common use cases and configurations are listed below, with further details about specific configuration settings in later chapters.

## Single Device SIP Paging

A common application of the 8190 is voice paging via SIP. SIP (Session Initiation Protocol) allows Algo IP products to register with most hosted/cloud or on-premise telephone systems to broadcast voice messages to multiple IP endpoints over a network in real-time.

The 8190 can be activated by dialing an assigned SIP extension from a telephone, device, or client. The speaker will auto-answer, play the default pre-announce tone, and allow voice paging until disconnected.

To do this, the 8190 must be registered as a SIP extension with a hosted or enterprise communications server. To register the 8190:

1. Open the 8190 web interface.
2. Navigate to the tab **Basic Settings** → **SIP**.
3. Enter the IP address, extension, username, and password for the SIP extension as a Page extension. This information will be available from the IT Administrator.

If VLAN is used, navigate to the **Advanced Settings** → **Network** tab to set VLAN options. Once the speaker is using VLAN you will need to be on the same VLAN to access the web interface.

Additional configurations can be made to meet the needs of the environment. This includes:

- Enabling the G.722 audio code for increased speech intelligibility
- Enabling ambient noise monitoring for the speaker volume to automatically adjust based on background noise
- Enabling talkback to allow those nearby the speaker to communicate with the caller

See SIP below for more details.

## Multiple Device SIP Paging using Multicast

Multicast is a method of transferring data from one transmitter device to multiple receiving devices simultaneously. To optimize the use of a single SIP extension, the 8190 can be used as a multicast transmitter to stream audio to other Algo receiver devices. Any number and combination of Algo speakers, paging adapters, or visual alerters can be set as receiving devices. Receiving devices do not require a unique SIP extension and, therefore, do not need to be registered with the SIP server.

In large environments, it is recommended that the device configured as the multicast sender be stored securely to mitigate the risk of interference or damage. The 8301 IP Paging Adapter and Scheduler is most often used in these scenarios.

In a smaller environment or when needed, the 8190 or other devices can also be configured as the multicast sender.

To enable multicast streaming to all receiving devices from the 8190:

1. Open the 8190 web interface.
2. Navigate to the tab **Basic Settings** → **Multicast**.
3. Under **Multicast Mode** select **Transmitter (Sender)**.
4. On the same tab, under **Transmitter Single Zone** select **All Call**.

The multicast addresses pre-populated in the table on the **Advanced Settings** → **Advanced Multicast** tab will work in most cases and should only be altered for rare cases.

To enable multicast receiving for other Algo devices:

1. Open the web interface for the device.
2. Navigate to the tab **Basic Settings** → **Multicast**.
3. Under **Multicast Mode** select **Receiver (Listener)**.
4. By default, receiving devices are set to monitor the **All Call** zone to receive multicast audio streaming.

Now, when a call is made via the 8190, receiving speaker devices will broadcast the page as well. Receiving speakers can independently configure volume and ambient noise monitoring.

Talkback can only be used for the SIP-registered speaker. The microphones in the receiver speakers are disabled except for the purpose of ambient noise monitoring.

See Multicast below for more details.

## Multiple Device SIP Paging using SIP Extensions

In cases where every speaker has a registered SIP extension, multicast may still be used to page multiple speakers simultaneously but each speaker remains able to be called individually or to generate a call when appropriately configured.

A speaker configured as a SIP-registered receiver will give highest priority to the **Priority Call** zone first, a page using the SIP extension next, and all multicast zones after.

When a call is made to the SIP extension, the 8190 can play a selected audio file before voice paging begins.

## Emergency Alerting

An emergency alert is a method of starting an audio file broadcast and looping the audio file until canceled. Algo IP devices come pre-loaded with audio files that can be used for alerts or custom files can be uploaded if desired.

There are two ways that audio files can be activated for emergency alerting applications:

1. Accessory Device (for example, pressing a call button)
2. SIP Call (for example, calling from an IP phone or UC platform).

## Using an Accessory Device for Emergency Alerts

Accessory devices like the Algo 1202 and Algo 1203 can be connected to a relay input port on an Algo IP endpoint to trigger emergency alerts when activated or pressed. In the web interface of the IP endpoint, the **Action When Input Triggered** can be configured under **Additional Features** → **Input/Output** to play an emergency tone.

## Using a SIP Call for Emergency Alerts

When Algo devices use SIP for emergency alerts, both a start trigger (**Announcement**) and stop trigger (**Call-to-Cancel**) must be configured. This allows users to activate an emergency alert and keep the phone available for use for other communications while the emergency alert is active.

When using SIP for emergency alerting, it is important to consider the options of using the phone keypad for DTMF codes or extensions. DTMF codes can be set for a single SIP extension on the multicast transmitter device and dialed to reach the desired DTMF page zone. When multiple extensions are used, each extension is mapped to a unique zone, allowing zones to be called directly.

| One Extension (DTMF) for Emergency Alerts | Multiple Extensions (Direct Dialing) for Emergency Alerts |
|---|---|
| Pros<br>• Only one extension or UC license needs to be registered, saving money<br>• Calls will be auto-answered and a confirmation tone can be played to provide feedback to the user<br>Cons<br>• Users must memorize DTMF keys individually, which can be challenging to recall | Pros<br>• Can set extensions as speed dials which requires less user training<br>• Option to use auto-answer or not.<br><br>With auto-answer: A confirmation tone can be played to provide feedback to the user<br><br>Without auto-answer: Can detect if the extension is part of a ring group and prevent interference with other calls or configurations such as loud ringing or other alerting<br>Cons<br>• Requires use of multiple extensions |

| | |
|---|---|
| | which increases overall cost |

See Emergency Alerts and Input/Output below for more configuration details.

## Loud Ringing

Loud ringing is configured using a SIP extension but is different from paging because a call is not answered and the line is not opened. Instead, a customizable recorded audio file is played.

Loud ringing can be configured for the 8190 to ensure the ring of a telephone can be heard even when ambient noise levels are high. To do this:

1. Open the 8190 web interface.
2. Navigate to the tab **Basic Settings** → **SIP**.
3. Enter the IP address, extension, username, and password for the SIP extension as a Ring extension. This information will be available from the IT Administrator.

## Bell Scheduling

The 8190 can play audio files for recurring alerts like school bells or shift changes when used with the 8301 IP Paging Adapter & Scheduler.

See the 8301 User Guide for more details.

## Poly Group Paging

The 8190 can be added to a Poly Group Page so that voice paging is heard over Poly telephone speakers and overhead paging simultaneously.

## VoIP, UC, or Mass Notification Platform Integration

Algo devices, including the 8190, can integrate with a variety of VoIP platforms including unified communication and mass notification platforms. This can be done via native configurations, SIP registration, or RESTful API.

As a Singlewire Solutions Partner, Algo products have been certified for compatibility and interoperability. To set up your device with Informacast, a license is required. An "-IC" version of the 8190 can be purchased with a license, or the license can be purchased separately. Once the license is acquired, use the web interface and navigate to **Advanced Settings** → **Admin** → **InformaCast**.

Algo devices are certified by and compatible with Microsoft Teams. When registered in the Microsoft Teams SIP Gateway, the 8190 can be configured to deliver Teams-based communication throughout facilities. To set up your device with Microsoft Teams, use the web interface and navigate to **Advanced Settings** → **Admin** → **Microsoft**.

For other UC platforms such as Zoom, RingCentral, and GoTo, or mass notification platforms such as Genetec, Intrado, and Raptor Technologies, the 8190 can integrate via SIP. To do this, use the web interface and navigate to **Basic Settings** → **SIP** to enter your SIP credentials.

See more compatible platforms.

## Custom Integrations

The Algo RESTful API enables custom integrations that do not rely on native compatibility or SIP registration.

When the Algo RESTful API is enabled, it can be used to access, manipulate, and trigger the 8190 on your network through HTTP/HTTPS requests. Requesting systems can interact with the 8190 predefined operations.

To configure API settings, use the web interface and navigate to **Advanced Settings** → **Admin** → **API Support**.

See the Algo RESTful API Guide for more details.

---

# Device Management

Algo IP devices can be managed and monitored both on-premise and remotely. The options of device management below help make device maintenance efforts more efficient by reducing the need to manually check devices individually to configure or troubleshoot.

## ADMP

The Algo Device Management Platform (ADMP) is a cloud-based device management solution to manage, monitor, and configure Algo IP endpoints from any location. Devices can be easily grouped via a tagging functionality, allowing devices to be coded by district, department, or function to easily oversee many devices. Devices can be supervised for connectivity and email-based notifications can be sent should devices go offline, allowing for a real-time overview of device status.

To connect your device to your ADMP account, use the web interface and navigate to **Advanced Settings → Admin → ADMP Cloud Monitoring**.

Note that if you choose to use ADMP to manage your devices, the Algo 8300 IP Controller cannot be used at the same time.

Learn more about ADMP.

## Algo 8300 IP Controller

The Algo 8300 IP Controller is designed for centralized on-premise Algo endpoint monitoring and supervision. Any Algo SIP endpoint device can be monitored on the network via the 8300 dashboard.

Note that if you choose to use the Algo 8300 IP Controller to manage your devices, ADMP cannot be used at the same time.

Learn more about the Algo 8300 IP Controller.

## SNMP

Simple Network Management Protocol (SNMP) can be used to monitor and manage your device from third-party tools that communicate via SNMP.

To configure your SNMP settings, use the web interface and navigate to **Advanced Settings → Admin → Simple Network Management Protocol**.

## RTCP

Real-Time Transport Control Protocol (RTCP) can be used to monitor data delivery.

To configure your RTCP settings, use the web interface and navigate to **Advanced Settings → Advanced Multicast → RTP Control Protocol (RTCP)**.

---

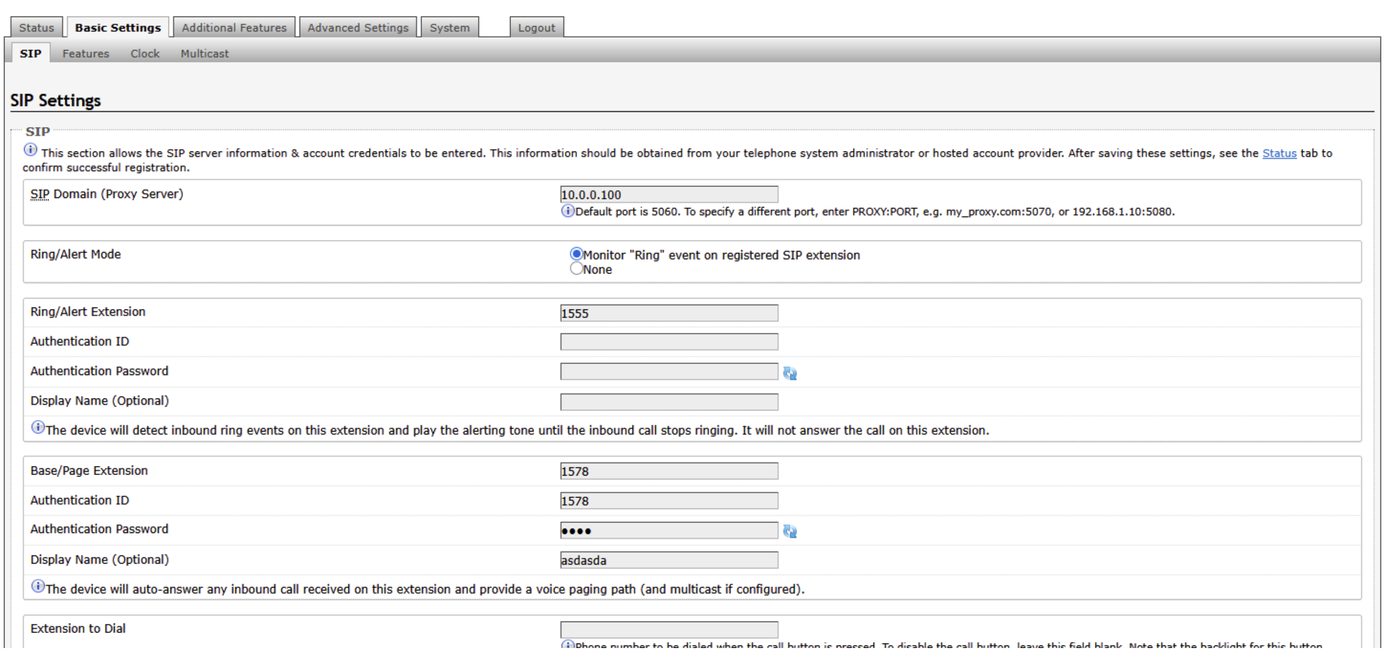
# SIP Configuration

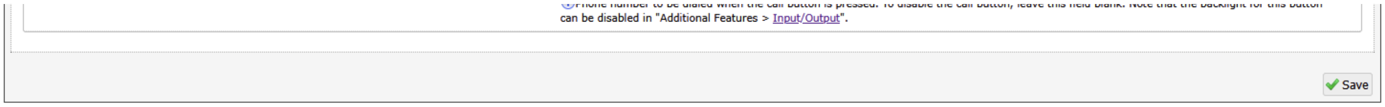
SIP (Session Initiation Protocol) is a common protocol use by most VoIP, UC, and other IP devices including Algo endpoints. Due to its reliability, SIP makes it easy to scale communication systems and integrate Algo IP devices with other technology.

For the 8190 to use SIP, a SIP license, account, and credentials are required. One license will be required per extension registered. If one device has multiple extensions registered, each registered extension will require a license. On a hosted or cloud platform, the required endpoint extension or seat may be treated the same as any other extension on the system and incur a monthly cost or similar fee.

## Basic Settings

Use these SIP settings to enter SIP server information and account credentials. For more details, ask your telephone system administrator or hosted account provider. After entering the information and saving the settings, check the Status tab to confirm the successful registration.






| SIP | |
|---|---|
| SIP Domain (Proxy Server) | The SIP Server's IP address (e.g., 192.168.1.111) or domain name (e.g., myserver.com). |
| Ring/Alert Mode | Ring extensions do not answer incoming calls but play a customizable, pre-recorded announcement, such as a loud ringer (night bell). Announcements are customizable and can be pre-recorded.<br><br>Use this setting to add a second SIP extension for a Ring event.<br>• **Monitor "Ring" event on registered SIP extension**<br>• **None: Default.**<br>When enabled, the device will detect inbound ring events on this extension and play the alerting tone (and multicast if configured) until the inbound call stops ringing. The 8190 will not answer the call on this extension.<br>Often, the 8190 will be a member of a hunt group or ring group to ring in conjunction with a telephone.<br><br>You may change the alert tone via **Basic Settings → Features.** |
| Ring Extension | Enter the SIP extension for the ring parameter of the 8190.<br><br>The device will detect inbound ring events on this extension and play the alerting tone (and multicast if configured) until the inbound call stops ringing. It will not answer the call on this extension. |
| Page Extension | Page extensions auto-answer and open a voice path, enabling live announcements.<br><br>Enter the SIP page extension for the 8190 so the device will auto-answer any inbound call received on this extension and provide a voice paging path (and multicast if configured). |

| | |
|---|---|
| Authentication ID | The Authentication ID is associated with the page extension. It is also referred to as 'Username' for some SIP servers. This may be the same as the Ring or Page extension in some cases. |
| Authentication Password | This is the SIP password for the registered SIP account used to authenticate SIP users.<br><br>Contact your System Administrator for the password. |
| Display Name (Optional) | Enter the name you want displayed when an SIP call is made. For the display name to be shown, the PBX and phone(s) must be configured to display this message as the Caller ID. |
| Extension to Dial | Phone number to be dialed when the call button is pressed. To disable the call button, leave this field blank. |

## More Page Extensions

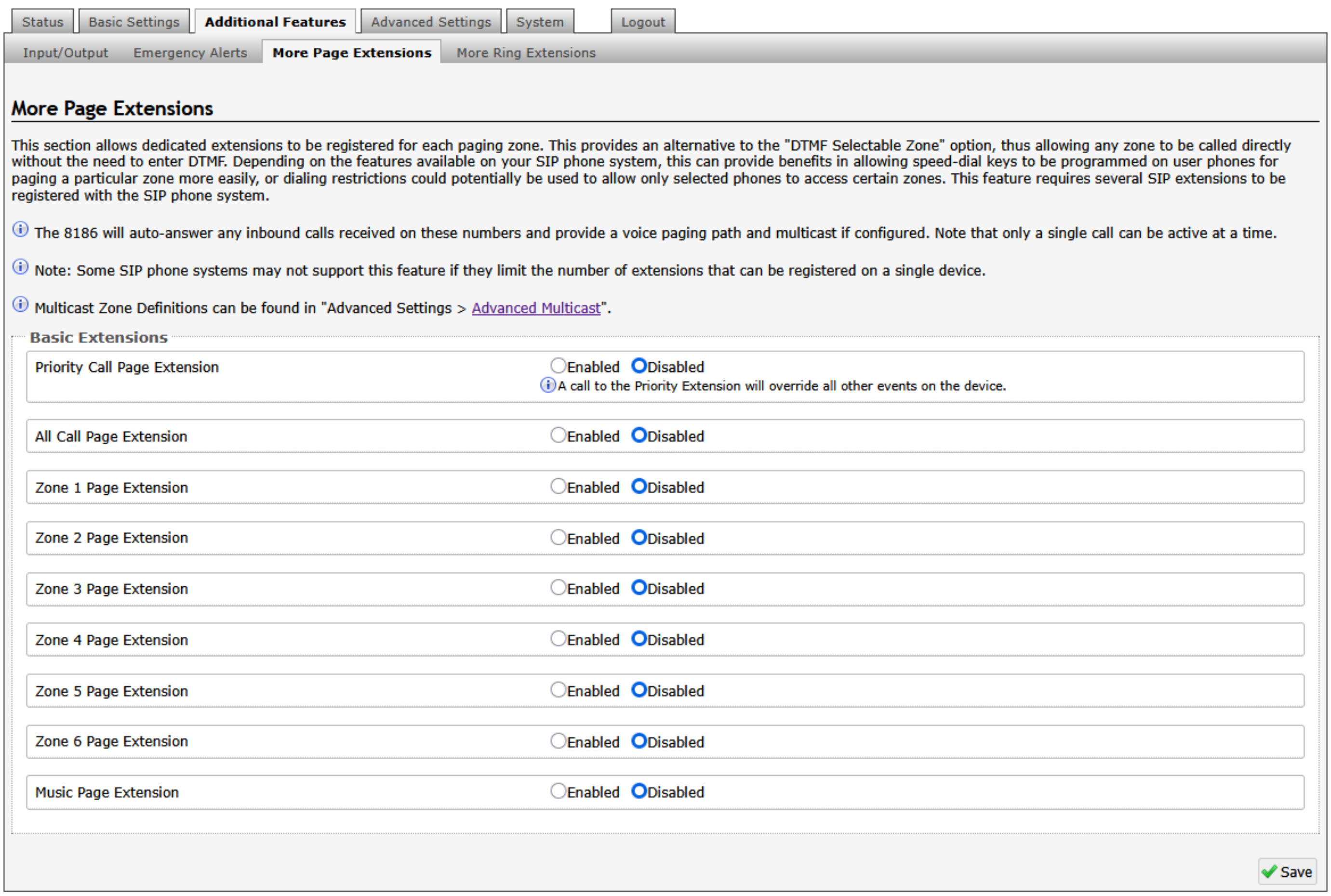
Using More Page Extensions is an alternative way to select several different multicast zones to page to when the device is configured as a multicast transmitter.

Additional SIP paging extensions can be registered for each multicast zone. This enables you to dial a zone directly without entering DTMF codes; however, this may require additional SIP licenses depending on the SIP provider. Some SIP telephone systems may not support this capability altogether if there is a limit on the number of extensions registered on a single device.

Some considerations when choosing to use multiple extensions over DTMF include:

| **DTMF (One Extension)** | **Multiple Extensions** |
|---|---|
| Pros<br>• Only one extension or UC license needs to be registered, saving money<br>• Calls can be auto-answered and a confirmation tone can be played to provide feedback to the user<br>Cons | Pros<br>• Can set extensions as speed dials which requires less user training<br>• Option to use auto-answer or not.<br><br>With auto-answer: A confirmation tone can be played to provide feedback to the user |

| | |
|---|---|
| • Users must memorize DTMF keys individually, which can be challenging to recall | Without auto-answer: Can detect if the extension is part of a ring group and prevent interference with other calls or configurations such as loud ringing or other alerting<br>Cons<br>• Requires use of multiple extensions which increases overall cost |




To configure additional page extensions (up to 50):

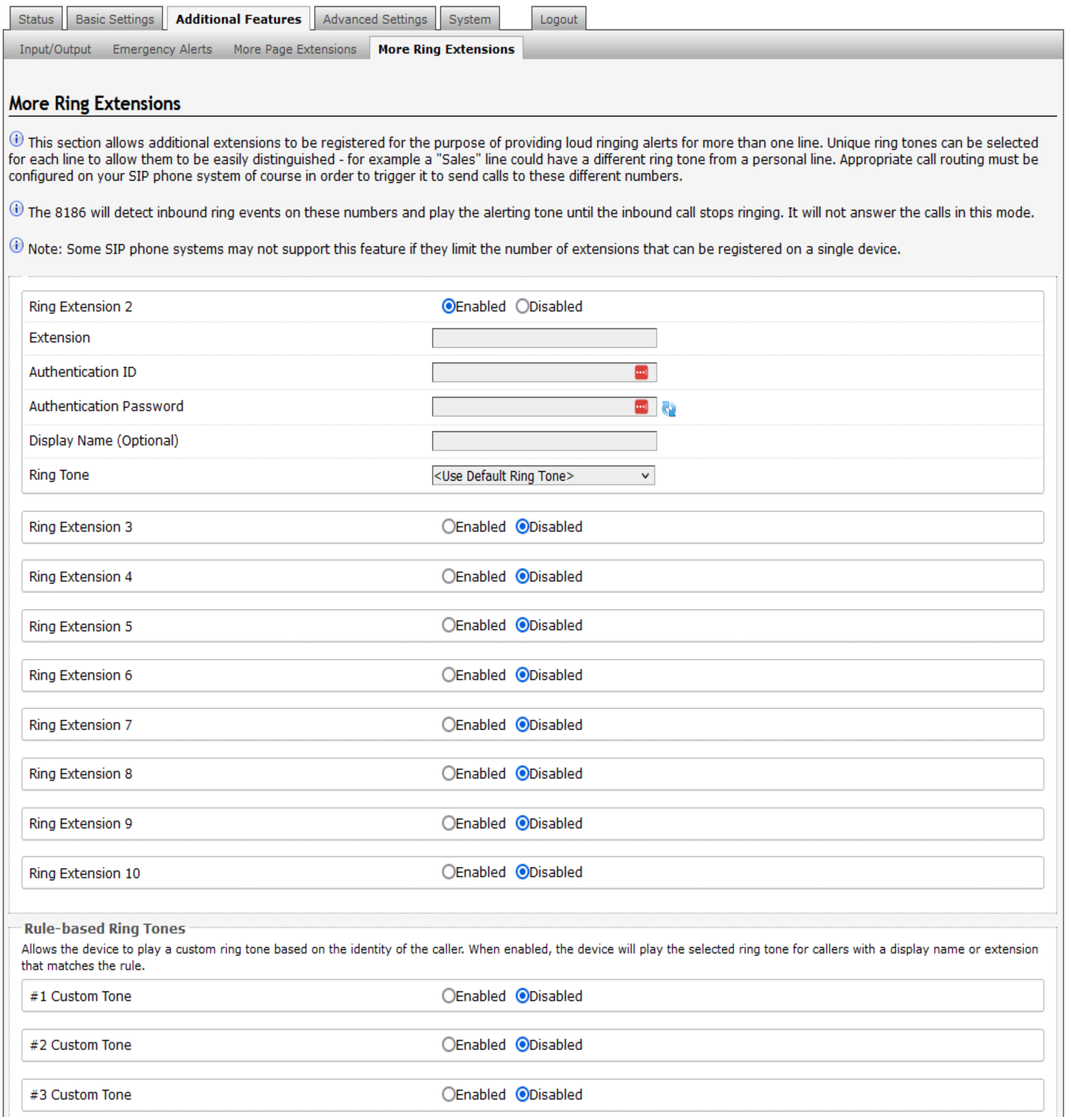
1. Select **Enable** beside the extension of interest.
2. Enter the **Extension**, **Authentication ID**, and **Authentication Password**. You may enter a display name if you'd like.

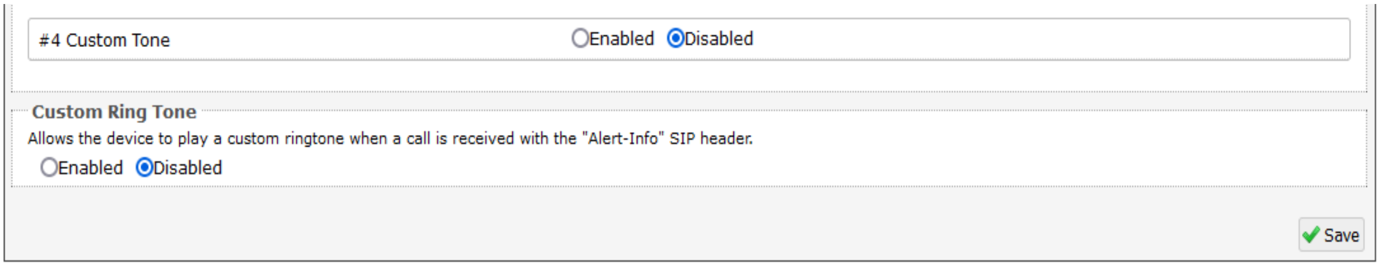
The 8190 will auto-answer any inbound calls received on these numbers, provide a voice paging path, and multicast to the associated multicast transmit zone if configured. Only a single call can be active at a time.

# More Ring Extensions

Additional ring extensions can be configured for other short term ring events, such as loud ringing. These should not be used for emergency alerts that are intended to be played indefinitely. For emergency alerts, see the Emergency Alerts tab. Using more ring extensions allows different ring tones to be played for each unique extensions to distinguish which phone is ringing.

Up to 10 SIP ring extensions can be registered.






To configure additional ring extensions, select **Enabled** beside an extension and enter the **Extension, Authentication ID,** and **Authentication Password**. If desired, a unique ringtone and multicast zone can be assigned to each extension.

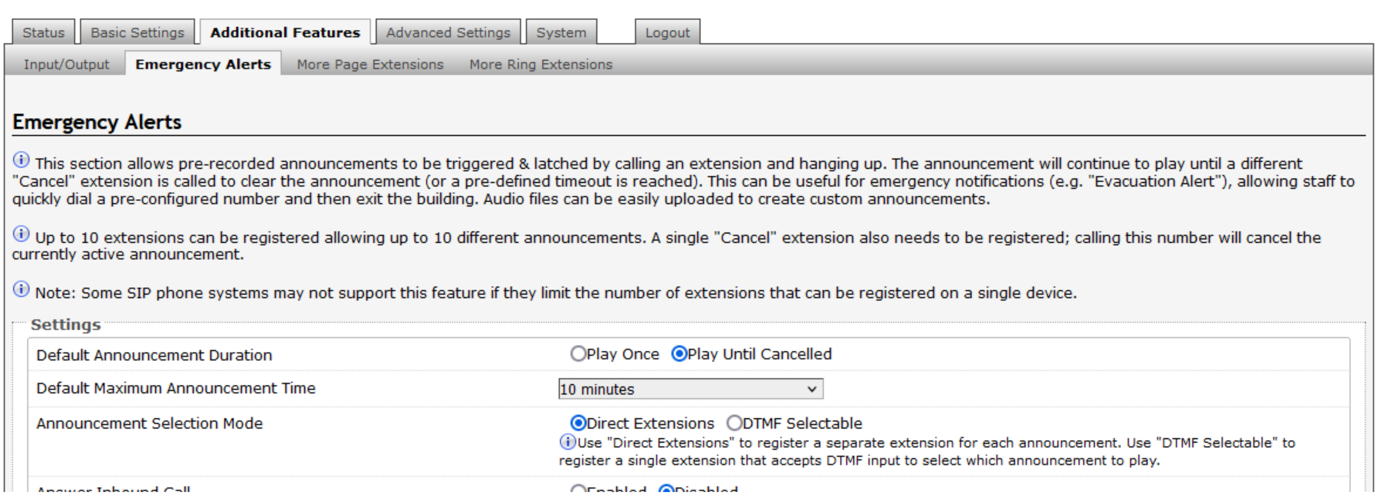
Set a rule-based ringtone for the device to play a custom ringtone based on the caller's identity. When enabled, the device will play the selected ringtone for callers with a display name or extension that matches the rule.

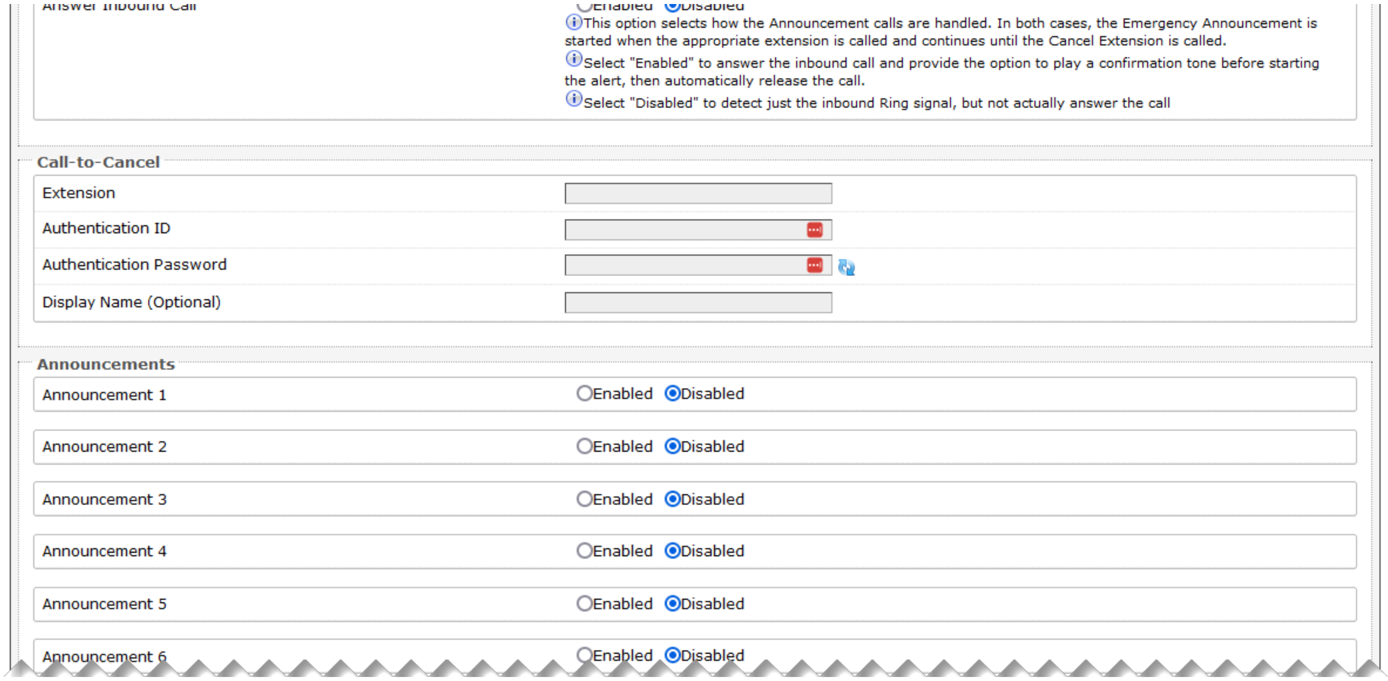
Enable a custom ring to allow the device to play a custom ringtone when receiving a call with the "Alert-Info" SIP header.

# Emergency Alerts

The 8190 can be used for alerting in the case of emergency (e.g., lockdown, evacuation, reverse evacuation), safety (e.g., medical, workplace accident), and security events (e.g., OSHA or similar workplace regulations).

Emergency alerts notify others of an emergency quickly and efficiently. Users can dial a pre-configured extension number to trigger and loop an emergency alert or announcement. Up to 10 extensions can be registered allowing up to 10 different announcements. A single “Call-to-Cancel” extension also needs to be registered. Calling this number will cancel an active announcement. Alternatively, DTMF can be used to cancel if the phone system being used does not support multiple extensions on the same device or if paying for multiple extensions is not within budget.






| **Settings** | |
|---|---|
| Default Announcement Duration | An announcement can be played once or continuously until canceled. Select **Play Once** to play a single cycle of the chosen tone file. If **Play Until Cancelled** is selected, the announcement will continue to play until the "Call-to-Cancel" extension is called to clear the announcement or a defined timeout is reached. |
| Default Maximum Announcement Time | Select the maximum time an announcement will play for. |
| Announcement Selection Mode | Select **Direct Extensions** to register a separate extension for each announcement. Select **DTMF Selectable** to register a single extension that accepts DTMF input to select which announcement to play. |
| Answer Inbound Call | Enable to answer inbound calls with the option to play a confirmation tone before starting an alert.<br>If disabled, the inbound ring signal will be detected, but the device will not answer the call. In some cases, keeping this setting disabled may be useful if the extension is part of a ring group. This will prevent interference with other calls or configurations such as loud ringing or other alerting. |

| | |
|---|---|
| Passcode Protected Announcement Extensions | Select **Enabled** to require the caller to enter a passcode after dialing an announcement or "Call-to-Cancel" extension. Setting a passcode helps prevent unintentional announcements. |
| Announcement Passcode | Enter a passcode that a caller must enter to play or cancel an announcement.<br>When prompted, the caller must enter the passcode followed by the # sign before the announcement will be played or canceled. The passcode prompt will be played before any other action. If the passcode is not correctly entered within 15 seconds, the call will end and there will be no change to the current announcement state. |
| Passcode Prompt Tone | Select a tone to play when the passcode is ready to be entered. |

| **DTMF Selection**<br>This extension will be used to activate and optionally cancel emergency alerts when **Announcement Selection Mode** is set to **DTMF Selectable**. Use the configurations below to register a single extension that will accept DTMF input to play selected announcements. | |
|---|---|
| Extension | Enter the SIP extension for the DTMF Selection parameter. |
| Authentication ID | Enter the Authentication ID. It may also be called Username for some SIP servers or may be the same as the extension. |
| Authentication Password | Enter the SIP password provided by the system administrator for the SIP account. |
| Display Name (Optional) | Enter a 'Display Name' that will be sent when the SIP call is made. The PBX and phone(s) must be configured to display this message as the Caller ID. |
| Prompt Tone | Select a tone to play when the passcode is ready to be entered. |

| **Call-to-Cancel** |
|---|

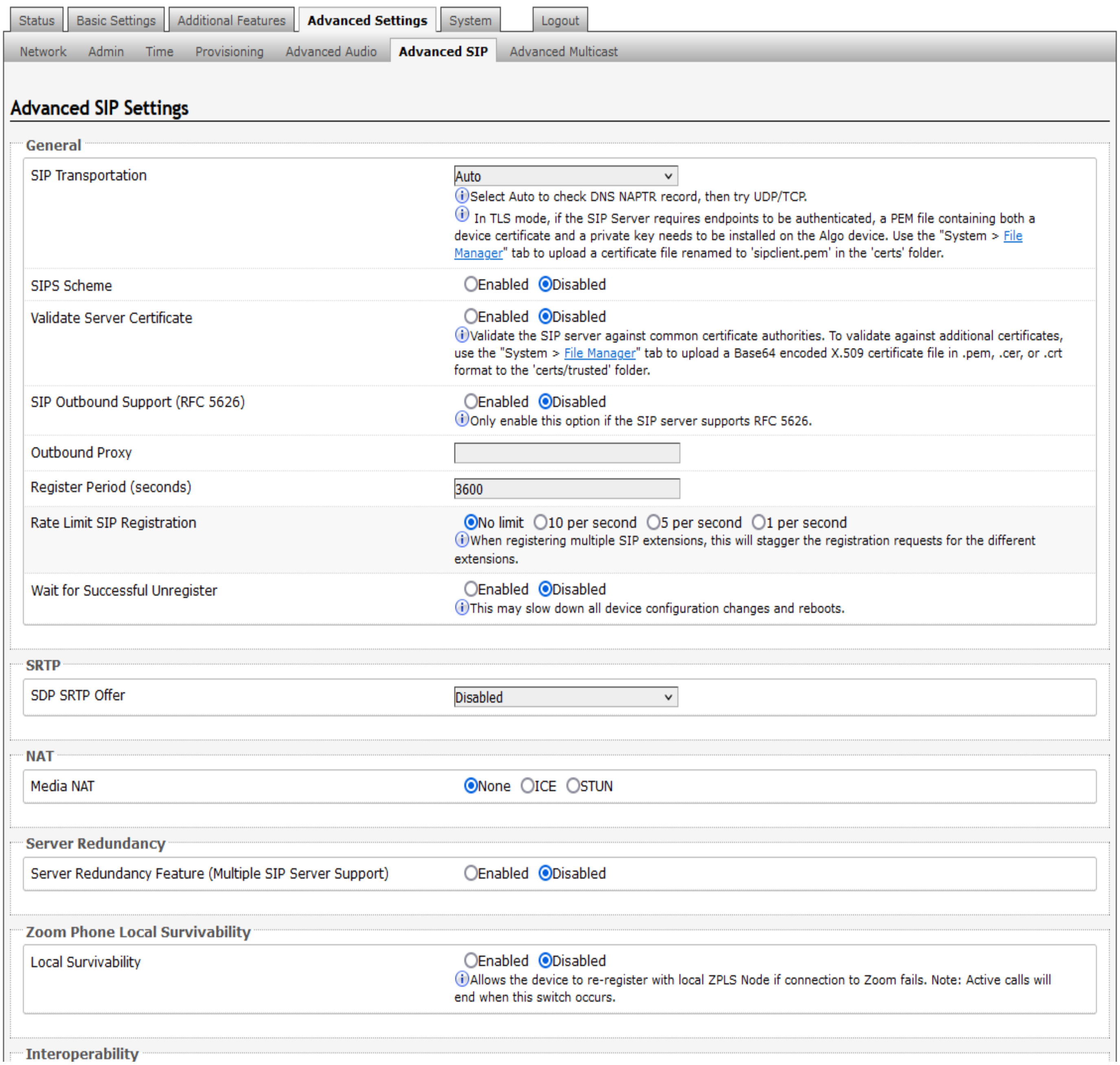
| | |
|---|---|
| Call-to-Cancel Selection Mode | If using "DTMF 0", the user should dial the main DTMF Selection extension and select '0' to cancel the announcement. Using DTMF 0 allows emergency alerts to work with only a single SIP registration rather than requiring multiple accounts. |
| Extension | Enter the SIP extension for the Call-to-Cancel Selection parameter. |
| Authentication ID | Enter the Authentication ID provided by the System Administrator. For some SIP servers, it may also be called the Username or the same as the extension. |
| Display Name (Optional) | Enter a display name that will be sent when the SIP call is made. The PBX and phone(s) must be configured to display this message as the Caller ID. |
| Confirmation Tone | Select a tone to play to confirm that an alert has been canceled. |

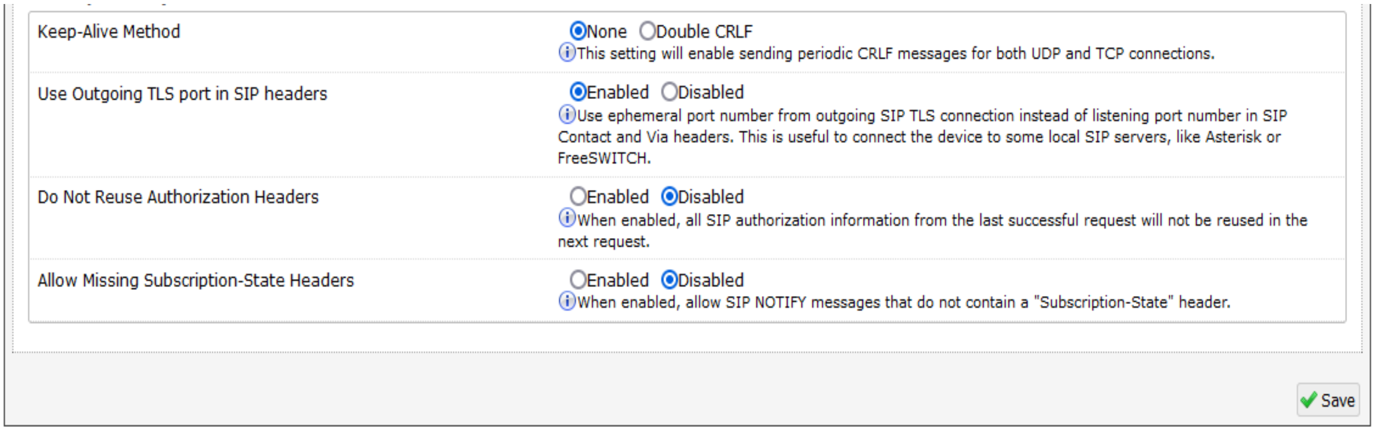
| **Announcements** | |
|---|---|
| Announcement # | To configure an Emergency Alert extension, select **Enabled** for an announcement number.<br>Up to 10 extensions can be registered allowing up to 10 different announcements. Audio files can be easily uploaded to create custom announcements. Only one 'Call-to-Cancel' extension is needed.<br>Alternatively, DTMF Selectable Mode can be used if the SIP telephone system limits the number of extensions that can be registered on a single device. |
| Announcement Duration | Choose the duration of an announcement. The **Default** option follows the behavior configured in **Default Announcement Duration**. |
| Maximum Announcement Time | Select the maximum announcement time. |
| Tone/Pre-recorded Announcement | Select a file to use as the announcement. |

| | |
|---|---|
| Confirmation Tone | Select a file to use as a confirmation tone. |
| Multicast Zone | Set the RTP multicast zone where announcements will be played. |
| Multicast Poly Group | Set the Poly Group where announcements will be played. |

# Advanced SIP

This section contains additional SIP configurations for more advanced features. These features may not be compatible with all SIP servers. Please consult your SIP Provider or IT team before making changes to these parameters






| **General** | |
|---|---|
| SIP Transportation | Select a transport layer protocol to use for SIP messages from the dropdown. These options include:<br>• **Auto**: Will check the DNS NAPTR record, then try UDP/TCP.<br>• **UDP**<br>• **TCP**<br>• **TLS**: Ensures the encryption of SIP traffic. In this mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key must be installed on the device. Upload a certificate via **System** → **File Manager** and rename it to 'sipclient.pem' in the 'certs' folder. |
| SIPS Scheme | Only visible when **SIP Transportation** is set to **TLS**. Enable to require the SIP connection from endpoint to endpoint to be secure. |
| Validate Server Certificate | Enable to validate the SIP server against common certificate authorities. To validate additional certificates, navigate to **System** → **File Manager** to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the **certs** folder. |
| SIP Outbound Support (RFC 5626) | Enable this option to support best networking practices according to RFC 5626. This option should be enabled if the device is registered with a hosted server or TLS is used for SIP Transportation. |

| | |
|---|---|
| | **Only enable this option if the SIP server supports RFC 5626.** |
| Outbound Proxy | Enter the IP address for an outbound proxy. |
| Register Period (seconds) | Enter the maximum requested period where the device will re-register with the SIP server. The default setting is 3600 seconds (1 hour).<br><br>Note that if the SIP response 200 (OK) provides an Expires header, this time will take precedence over the **Register Period** defined time here.<br><br>Only change if instructed to do so. |
| Rate Limit SIP Registration | This option should be used in cases where many SIP extensions are registered (ex. one for each zone).<br>Select a rate limit to stagger registration requests and prevent overloading the server by sending them all at the same time. |
| Wait for Successful Unregister | Enable to wait for the device to successfully unregister from the server. Enabling may cause a slight delay during configuration changes and reboots |

| **SRTP** | |
|---|---|
| SDP SRTP Offer | Select an option from the dropdown menu:<br>• **Disabled**<br>• **Standard**: Encrypts RTP voice data to secure audio RTP packets (SRTP). SIP calls will be rejected if the other party does not support SRTP. This option secures the audio data between parties by ensuring that it's not left out for third parties to reconstruct and listen to.<br>• **Optional** (Non-standard AVP Profile): If the other party does not support SRTP, the SIP call's RTP data will be unencrypted. |
| SDP SRTP Offer Crypto Suite | The encryption and authentication algorithms used for voice data. |

| NAT | |
|---|---|
| Media NAT | IP address for STUN server if present or IP address/ credentials for a TURN server. |
| ICE – TURN Server | Enter the IP address or domain of the ICE server. |
| ICE – TURN User | Enter the username. |
| ICE – TURN Password | Enter the password. |
| STUN - Server | Enter the IP address or domain of the STUN server. |

| Server Redundancy | |
|---|---|
| Server Redundancy Feature | Enable to configure up to two secondary backup servers.<br><br>When enabled, the device will attempt to register with the primary server but switch to a secondary server when necessary. The configuration allows re-registration to the primary server upon availability or to stay with a server until unresponsive. |
| Backup Server #1, #2 | Provided by your SIP provider or IT team. |
| Polling Intervals (seconds) | Select the time interval for sending monitoring packets to each server from the dropdown menu. Inactive servers are always polled and the active server may optionally be polled. |
| Poll Active Server | Enable to explicitly poll the current server to monitor availability. Other regular events may also handle this automatically and can be disabled to reduce network traffic. |
| Automatic Fallback | Enable to allow the device to reconnect with a higher priority server once available, even if the backup connection is still working. |
| Polling Method | Select a polling method based on what your SIP provider supports. |

| Zoom Phone Local Survivability |
|---|

| | |
|---|---|
| Local Survivability | Enable to re-register with local ZPLS Node if connection to Zoom fails. This allows sites to maintain a subset of Zoom Phone features even if connectivity to the Zoom Phone cloud is lost. |
| Survivability Proxy | The IP address or domain name of the local ZPLS node. |

| **Interoperability** | |
|---|---|
| Keep-Alive Method | Select a keep-alive method:<br>• **None**<br>• **Double CRLF**: The device will send a packet regularly to maintain connection with the SIP Server if behind NAT. |
| Keep-Alive Interval (seconds) | Set the interval in seconds that the CRLF message should be sent. 30 seconds is recommended. |
| Use Outgoing TLS port in SIP Headers | Enable to use the ephemeral port number from an outgoing SIP TLS connection instead of the listening port number in SIP Contact and Via headers. This is useful for connecting the device to some local SIP servers, like Asterisk or FreeSWITCH. |
| Do Not Reuse Authorization Headers | Enable so all SIP authorization information from the last successful request will not be reused in the next request. |
| Allow Missing Subscription-State Headers | Enable to allow SIP NOTIFY messages that do not contain a 'Subscription-State' header. |

# Multicast Configuration

The 8190 can be programmed as a multicast transmitter or receiver and can be grouped into up to 50 multicast zones. Multicast is a method of transferring data from one transmitter device to multiple receiving devices simultaneously. To optimize the use of a single SIP extension, the 8190 can be used as a multicast transmitter to stream audio to other Algo receiver devices. Any number and combination of Algo speakers, paging adapters, or visual alerters can be set as receiving devices. Receiving devices do not require a unique SIP extension and therefore do not need to be registered with the SIP server.

In large environments, it is recommended that the device configured as the multicast sender be stored securely to mitigate risk of interference or damage. The 8301 IP Paging Adapter and Scheduler is most often used in these scenarios. In a smaller environment or when needed, the 8190 or other devices can also be configured as the multicast sender.

When multiple zones are used, they can be called via DTMF (single extension) or multiple SIP extensions. DTMF codes can be set for a single SIP extension on the transmitter device and dialed to reach the desired DTMF page zone. When multiple SIP extensions are used, each extension is mapped to a unique zone, allowing zones to be called directly.

# Multicast IP Addresses

Each 8190 has a unique IP address and shares a common multicast IP and port number (multicast zone) for multicast packets. The transmitter units send to a configurable multicast zone, and the Receiver units listen to assigned multicast zones.

The network switches and router see the packet and deliver it to all the zone members. The multicast IP and port number must be the same on all transmitter and receiver units of the same zone. The user may define multiple zones by picking different multicast IP addresses and/or port numbers.

1. Multicast IP addresses range: 224.0.0.0/4 (from 224.0.0.0 to 239.255.255.255)
2. Port numbers range: from 1 to 65535
3. By default, the 8190 is set to use the multicast IP address 224.0.2.60 and the port numbers 50000-50008

Ensure the multicast IP address and port number do not conflict with other services and devices on the same network.

# Enable Multicast Streaming

The 8190 multicast features only require the first endpoint be registered as a SIP extension. Only one audio stream can be active and sent to additional Algo IP endpoints, including any combination of paging adapters, speakers, and visual alerters, may be added as multicast receivers. If multiple unique audio streams are needed simultaneously, more than one transmitter will be required. If multiple unique audio streams are needed simultaneously, more than one transmitter will be required.

The Algo IP endpoint configured as the transmitter will stream audio to all of the receivers simultaneously. Receiver endpoints do not require SIP extensions and do not need to register with the SIP communication server.

To enable multicast streaming from the transmitter adapter, open the web interface and go to the **Basic Settings** → **Multicast** tab. For Multicast Mode, select **Transmitter (Sender)**. For Transmitter Single Zone, select **All Call** or other zones as desired.

To enable multicast monitoring of the receiver endpoints, go to the web interface for each endpoint and navigate to the **Basic Settings** → **Multicast** tab. For Multicast Mode, select **Receiver (Listener)**. The endpoint will monitor the **All Call** zone IP address by default as well as any other zones assigned under **Basic Receiver Zone**.

The page pre-announce tone is generated from the transmitter. The speaker volume can be increased or decreased for each multicast receiver individually.

## Using Multicast Page Zones

By default, the 8190 can listen to nine basic multicast zones, however, up to 50 are available (See **Additional Features** → **More Page Extensions** for more details). The multicast IP addresses define these zones.

By default these zones have the names below but can be used however you prefer:

- Priority
- All Call
- Zone 1
- Zone 2
- Zone 3
- Zone 4
- Zone 5
- Zone 6
- Music

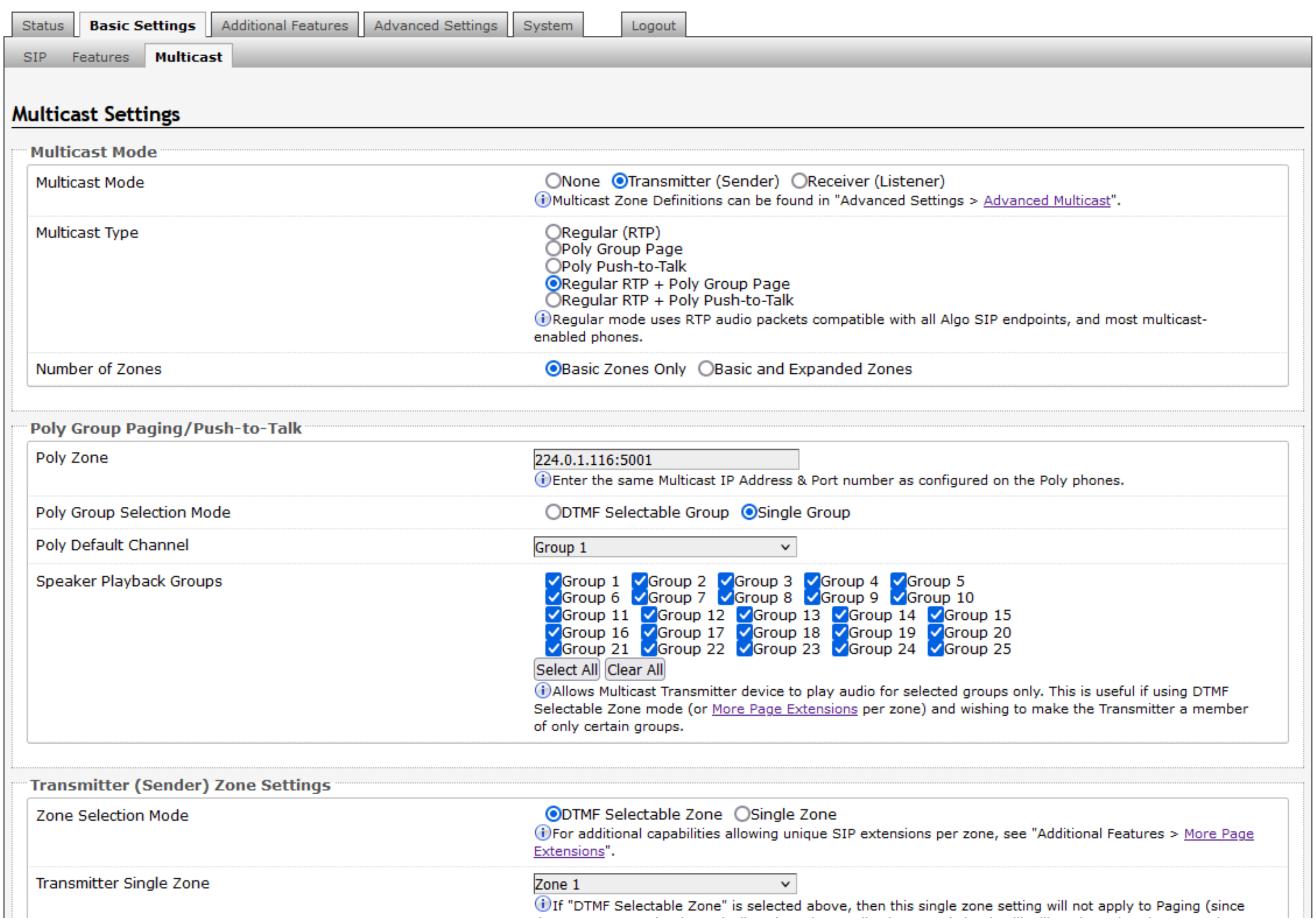
When set as a multicast receiver, zones have a priority hierarchy where zones higher on the list will be treated with higher priority, with **Music** being the lowest priority. When set as a multicast transmitter, event priority is based on the event type that initiated the multicast rather than the output multicast channel that will be active.

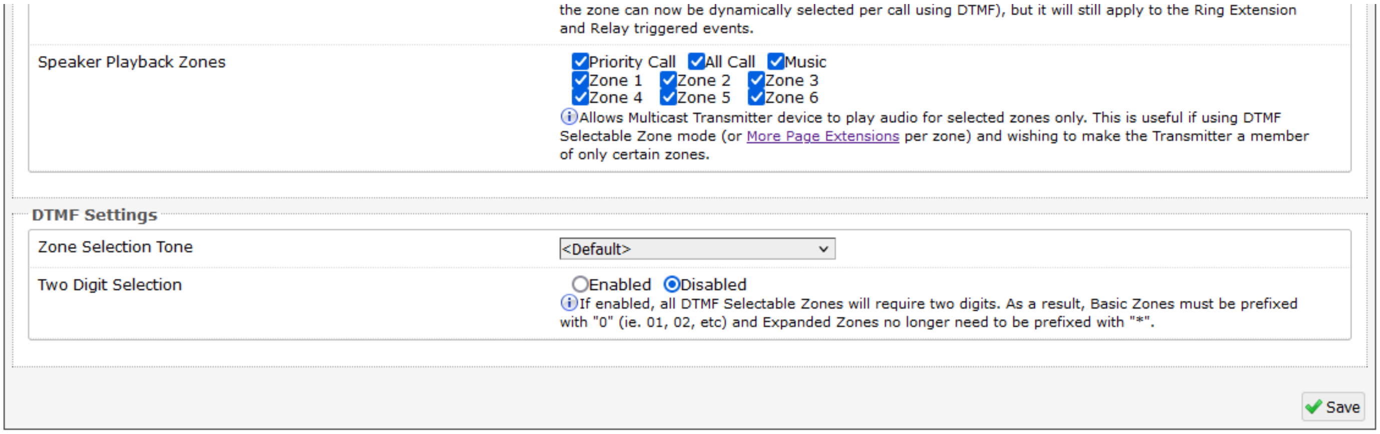
There are two options for paging to multiple zones:

1. DTMF Selectable Mode: Has a dynamic page zone selection and requires only the transmitting device to have a registered SIP extension. To page, dial the SIP extension of the transmitter and dial the desired DTMF page zone (e.g., 1, 2, etc.) on the keypad. DTMF digits and their corresponding zone numbers can be found in the **Advanced Settings** → **Advanced Multicast** tab of the 8190 web interface.
2. Multiple page extensions: Multiple SIP extensions can be registered on the transmitter. Each extension is mapped to a unique zone, allowing zones to be called directly. See **Additional Features** → **More Page Extensions** tab of the 8190 web interface for more details.

# Multicast: Transmitter (Sender)

Always ensure that the multicast settings (such as zone numbers, the multicast IP address, and port definitions) on all receiver devices match those of the transmitter device.






| **Multicast Mode** | |
|---|---|
| Multicast Mode | If **Transmitter (Sender)** is selected, the 8190 will broadcast an IP stream when activated in addition to playing audio. The 8190 cannot be both a multicast Transmitter and Receiver simultaneously. |
| Multicast Type | The 8190 may broadcast multicast paging compatible with Poly “on-premise group paging” protocol and most multicast-enabled phones that use RTP audio packets.<br><br>Select **Regular (RTP)** if you are only multicasting to Algo IP endpoints or multicast-enabled phones.<br>To multicast page announcements to Poly phones, select **Poly Group Page** or **Poly Push-to-Talk**.<br><br>Select **Regular RTP + Poly Group Page** or **Regular RTP + Push-to-Talk** to multicast page audio to Poly phones, Algo IP endpoints, and multicast-enabled phones. |
| Number of Zones | Select **Basic Zones Only** if configuring nine or fewer multicast zones. Select **Basic and Expanded Zones** to configure up to 50 zones. The expanded zones have the same behavior as the basic Receiver zones but are hidden by default to simplify the interface. |

| **Poly Group Paging/Push-to-Talk**<br>This section is used if the Multicast Type includes Poly Group Page or Poly Push-to-Talk. | |
|---|---|
| Poly Zone | Enter the same Multicast IP Address and Port number configured on the Poly phones. |
| Poly Group Selection Mode | Select **Single Group** to broadcast on one pre-configured group. Multiple SIP extensions can be registered on the Transmitter device. Each extension is mapped to a unique group, allowing groups to be called directly (e.g., from speed-dial keys). See **Additional Features → More Page Extensions** for additional configuration settings.<br><br>If **DTMF Selectable Group** is selected, the group is determined by the DTMF selection between 0 – 25.<br>To page using DTMF Selectable Zone:<br>1. Dial the SIP extension of the Transmitter device<br>2. Dial the desired DTMF page group number on the keypad when prompted. Groups 10 and higher start with "*".<br>DTMF group definitions include:<br>• DTMF Extension 1 for Zone 1<br>• DTMF Extension 2 for Zone 2<br>...<br>• DTMF Extension ∗10 for Zone 10<br>• DTMF Extension ∗11 for Zone 11<br><br>All DTMF codes and respective zones are available in **Advanced Settings → Advanced Multicast**. |
| Poly Default Channel | Select the default group for the multicast stream to be sent to. **If DTMF Selectable Group** is chosen, this single group setting will not apply to paging since the group will be dynamically selected per call using DTMF. The **Single Group** setting will still apply to the ring extension and relay triggered events. |

| | |
|---|---|
| | The **Poly Default Channel** is the default channel used for multicast actions unless an option is available for a custom channel with specific parameters. |
| Speaker Playback Groups | Select Speaker Playback Groups to control which specific groups can play audio from the device. This is useful if using the **DTMF Selectable Group** mode or additional page extensions (**Additional Features** → **More Page Extensions**) per group to make 8190 a member of only certain zones. In this case, the Transmitter does not participate in the Zone but transmits certain traffic. |

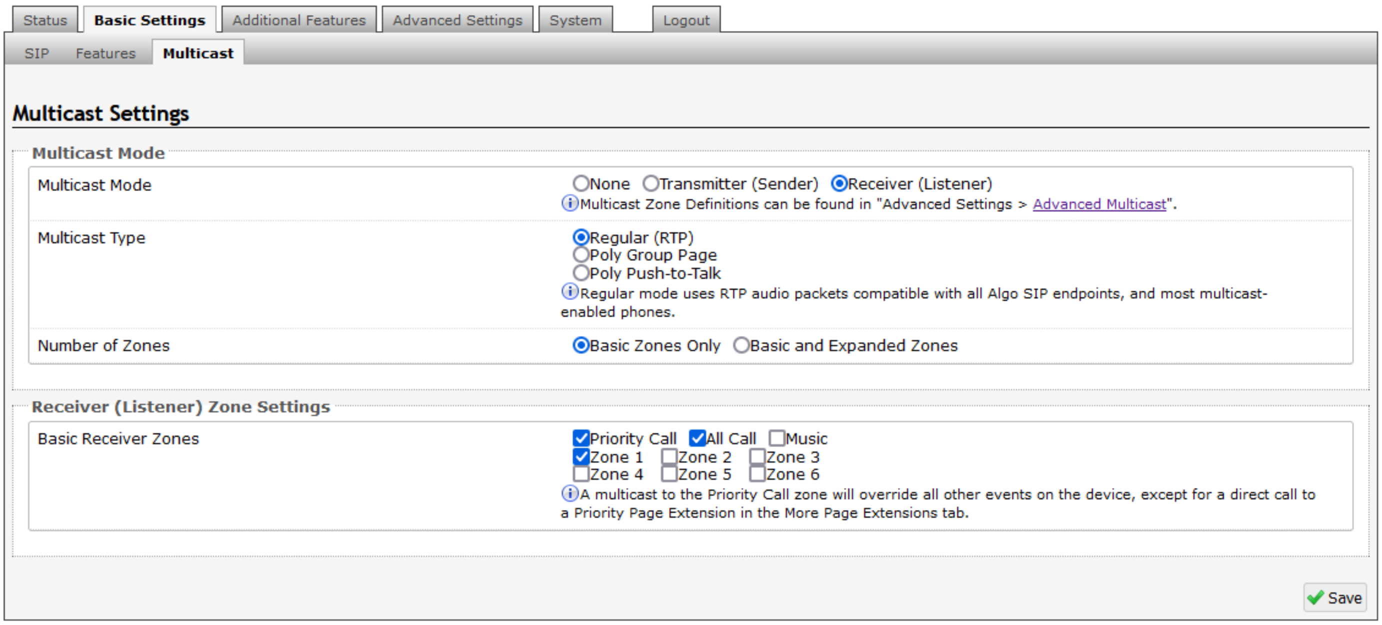
| **Transmitter (Sender) Zone Settings**<br>This section is used if the Multicast Type includes Regular (RTP). | |
|---|---|
| Zone Selection Mode | Select **Single Zone** to broadcast on one pre-configured zone. Multiple SIP extensions can be registered on the Transmitter device. Each extension is mapped to a unique zone, allowing zones to be called directly (e.g., from speed-dial keys). See **Additional Features** → **More Page Extensions** for additional configuration settings.<br><br>If **DTMF Selectable Zone** is selected, the zone is determined by the DTMF selection between 0 – 50. Once multicast Transmitter mode is enabled, navigate to **Advanced Settings** → **Advanced Multicast** to find the DTMF codes corresponding to each zone.<br><br>To page using **DTMF Selectable Zone:**<br>1. Dial the SIP extension of the Transmitter device<br>2. Dial the desired DTMF page zone number on the keypad when prompted. Zones 10 and higher start with "*". DTMF zone definitions include:<br>• DTMF Extension 9 for Priority Call<br>• DTMF Extension 0 or 8 for All Call<br>• DTMF Extension 1 for Zone 1<br>• DTMF Extension *10 for Zone 10 |

| | |
|---|---|
| | • DTMF Extension ∗11 for Zone 11<br><br>All DTMF codes and respective zones are available in **Advanced Settings → Advanced Multicast**. |
| Transmitter Single Zone | Select the default zone for the multicast stream to be sent to. The Transmitter Single Zone is the default zone used for multicast actions unless an option is available for a custom zone with specific parameters.<br><br>If **DTMF Selectable Zone** is chosen, this single zone setting will not apply to paging since the zone will be dynamically selected per call using DTMF. However, this single zone setting will still apply to the ring extension and relay-triggered events. |
| Speaker Playback Zones | Select Speaker Playback Zones to control which specific zones the 8190 can play audio for. This is useful if using the DTMF Selectable Zone mode or additional page extensions (**Additional Features → More Page Extensions**) per zone to make the 8190 a member of only certain zones. In this case, the transmitter does not participate in the zone but can still send audio to speakers in different zones. |

**DTMF Settings**
This section is used if the Zone Selection Mode is set to DTMF Selectable Zone.

| | |
|---|---|
| Zone Selection Tone | Select a tone to be played to prompt a user to select a zone to multicast to.<br><br>This may be used as an interactive voice response (IVR) menu by uploading a custom audio file in the **tones** folder through **System → File Manager**. Each zone may use a different tone. This can be configured in **Advanced Settings → Advanced Multicast**. |
| Two-Digit Selection | When enabled, all DTMF Selectable Zones will require two digits. As a result, Basic Zones must be prefixed with *0*, and Expanded Zones will no longer need to be prefixed with *. |

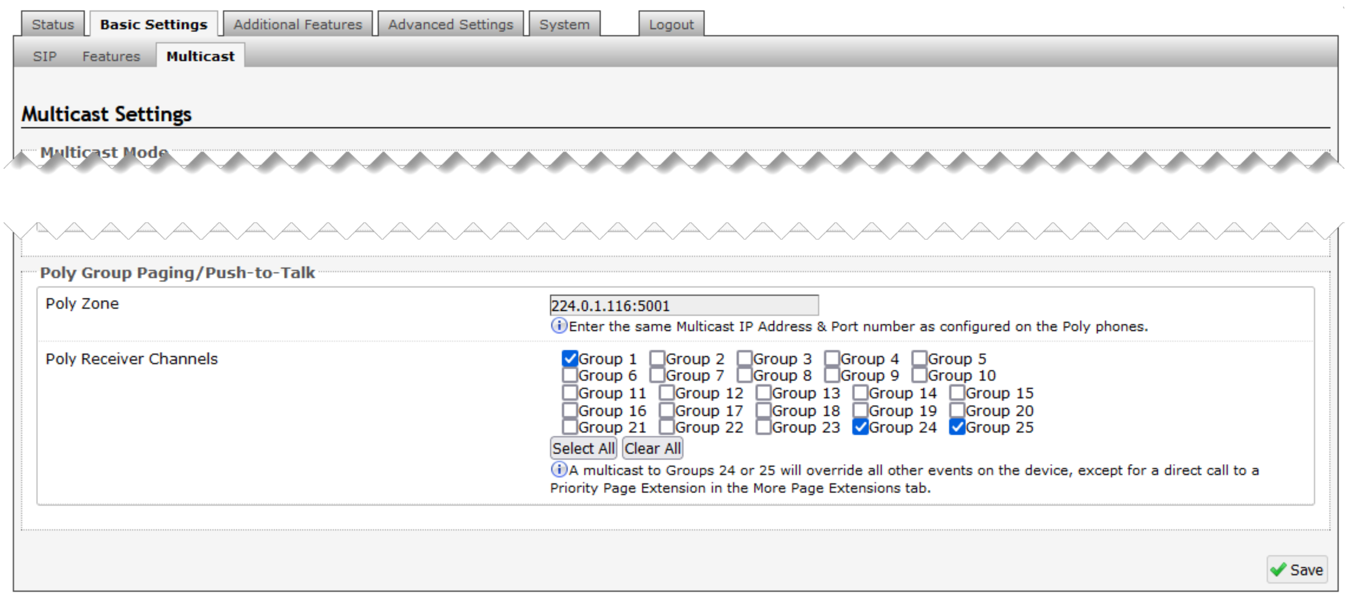
# Multicast: Receiver (Listener)




| **Multicast Mode**<br>Always ensure that the multicast settings on all Receiver devices match those of the Transmitter. | |
|---|---|
| Multicast Mode | If **Receiver (Listener)** mode is selected, the 8190 will activate when receiving a multicast audio stream. It will mimic the audio stream of the transmitter but use local volume settings. This can be set via **Basic Settings** → **Features** → **Page Speaker Volume**. |
| Multicast Type | Select **Regular** if receiving multicast from other Algo IP endpoint(s) and/or multicast-enabled phone(s) that use RTP audio packets.<br><br>Select **Poly Group Page** or **Poly Push-to-Talk** if receiving multicast paging compatible with Poly “on-premise group paging” protocol. |
| Number of Zones | Select **Basic Zones Only** if configuring nine or fewer multicast zones. Select **Basic and Expanded Zones** to configure up to 50 zones. The expanded zones have the same behavior as the basic Receiver zones but are hidden by default to simplify the interface. |

| Receiver (Listener) Zone Settings | |
|---|---|
| Basic Receiver Zones | Select one or more multicast zones for the 8190 to listen to. Multicast zone priority will be based on the zone definition list order defined in **Advanced Settings → Advanced Multicast**. |
| Expanded Receiver Zones | Select additional zones (up to 50) for the device to listen to. This is only possible when **Basic and Expanded Zones** is selected. |

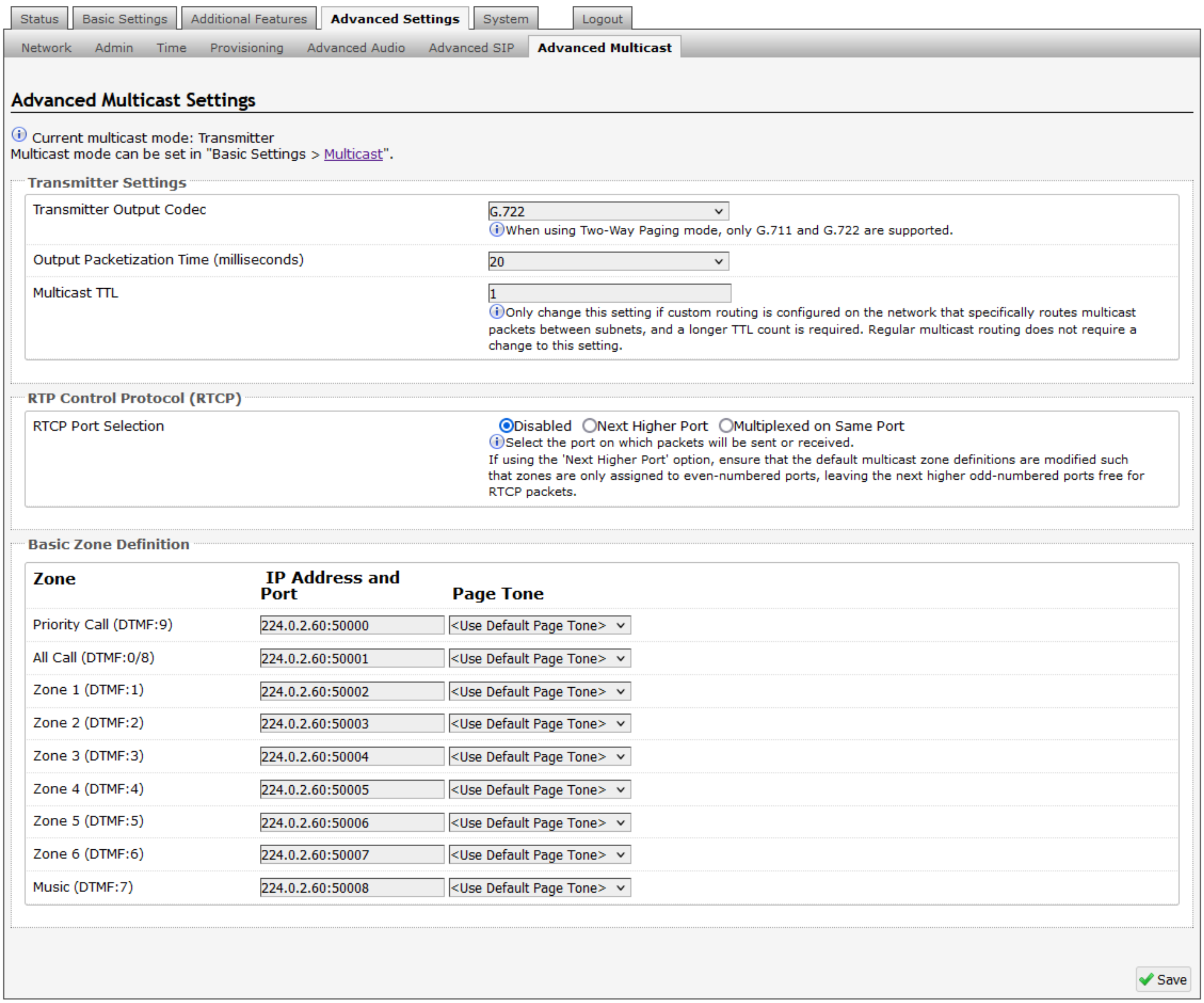
**Poly Group Paging/Push-to-Talk**




| | |
|---|---|
| Poly Zone | Enter the Poly Zone (IP Address and Port) that matches the configuration of the Poly phones and Channels. |
| Poly Receiver Channels | If using a Poly telephone as a Multicast Transmitter, a tone may be set for any of the 25 Poly Groups configured on the 8190. Poly Group Tones can be set in **Advanced Settings → Advanced Multicast**.<br><br>The Poly telephone used as a page audio source for the 8190 must be configured to use either the G.711 or G.722 audio codec.<br><br>Note that Poly phone(s) must be configured with the “Compatibility” setting (“ptt.compatibilityMode”) disabled for this codec setting to be applied. |

# Advanced Multicast

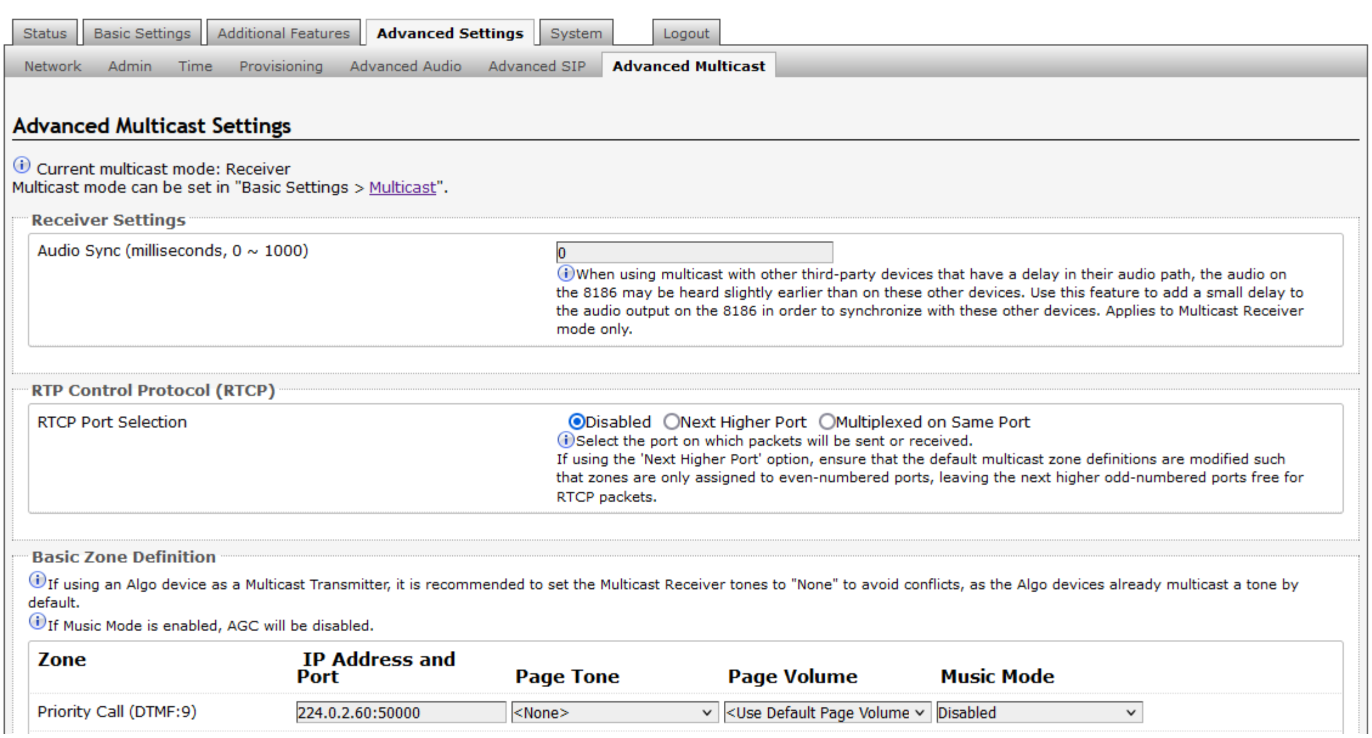
These settings are only visible when in Transmitter or Receiver multicast mode. This can be set in **Basic Settings** → **Multicast**. The default pre-populated multicast zone IP addresses and ports will work in most cases and should only be altered for rare cases.

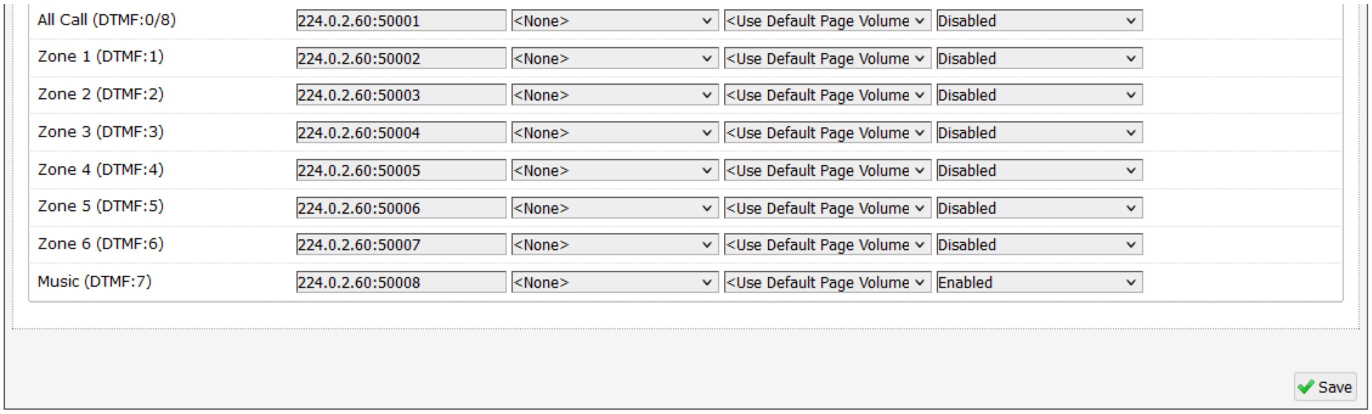



| Transmitter Settings | |
|---|---|
| Transmitter Output Codec | Select an audio encoding format for the Transmitter device to use when sending output to the Receivers. Supported formats include:<br>• G.711 ulaw<br>• G.722<br>• Opus<br>• L16 |

| | |
|---|---|
| | Only G.711 and G.722 are supported when using Two-Way Paging mode. |
| Output Packetization Time (milliseconds) | Select the size of the audio packets the Transmitter sends to the Receivers from the dropdown menu. The default of 20 milliseconds is recommended unless a different value is specifically required for compatibility with other devices. |
| Multicast TTL | Only change the multicast time to live (TTL) setting if custom routing is configured on the network that specifically routes multicast packets between subnets and a longer TTL count is required. This ensures packets are not bounced back and forth in a network indefinitely. When the TTL is reached, the router drops the packet. |

| **RTP Control Protocol (RTCP)** | |
|---|---|
| RTCP Port Selection | Select how a port will be chosen to send or receive RTCP packets.<br><br>Note: If **Next Higher Port** is selected, ensure that the default multicast zone definitions are modified so that zones are only assigned to even-numbered ports, leaving the next higher odd-numbered ports free for RTCP packets. |





| | | | | |
|---|---|---|---|---|
| All Call (DTMF:0/8) | 224.0.2.60:50001 | <None> | <Use Default Page Volume | Disabled |
| Zone 1 (DTMF:1) | 224.0.2.60:50002 | <None> | <Use Default Page Volume | Disabled |
| Zone 2 (DTMF:2) | 224.0.2.60:50003 | <None> | <Use Default Page Volume | Disabled |
| Zone 3 (DTMF:3) | 224.0.2.60:50004 | <None> | <Use Default Page Volume | Disabled |
| Zone 4 (DTMF:4) | 224.0.2.60:50005 | <None> | <Use Default Page Volume | Disabled |
| Zone 5 (DTMF:5) | 224.0.2.60:50006 | <None> | <Use Default Page Volume | Disabled |
| Zone 6 (DTMF:6) | 224.0.2.60:50007 | <None> | <Use Default Page Volume | Disabled |
| Music (DTMF:7) | 224.0.2.60:50008 | <None> | <Use Default Page Volume | Enabled |

Save

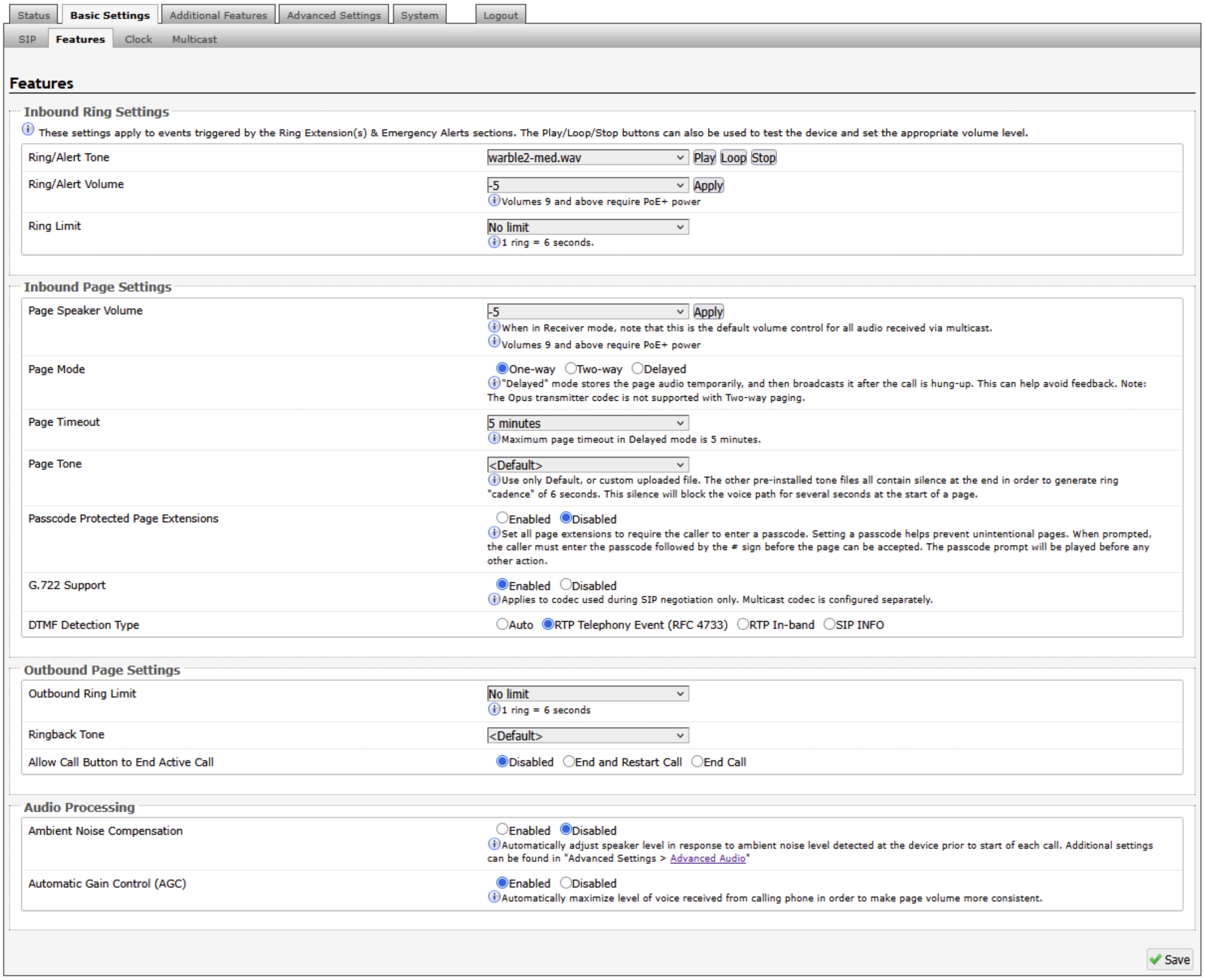
| Receiver Settings | |
|---|---|
| Audio Sync | Available if under **Basic Settings** → **Multicast** the **Multicast Mode** is set to **Receiver (Listener)** and **Multicast Type** is set to **Poly Group Page** or **Poly Push-to-Talk**. When using multicast with other third-party devices that have a delay in their audio path, the audio on the 8190 may be heard slightly earlier than on these other devices.<br><br>Use this feature to add a small delay on the 8190 to synchronize with these other devices. |

| Poly Receiver Tones | |
|---|---|
| Poly Receiver Tones | Available if under **Basic Settings** → **Multicast** the **Multicast Mode** is set to **Receiver (Listener)** and **Multicast Type** is set to **Poly Group Page** or **Poly Push-to-Talk**. A tone may be set for any of the 25 Poly Groups. If using an Algo device as a Multicast Transmitter, it is recommended to set the Receiver tones to **None** to avoid conflicts, as the Algo devices already multicast a tone by default. |

# Audio Configuration

Audio configurations for the 8190 include ring settings, page settings, audio processing, emergency alerts, tones, and much more. Use the sections below to understand how each configuration works for audio output and control best suited for the device's environment.

# Basic Settings & Features




**Inbound Ring Settings**

Ring settings apply to events triggered by Ring Extensions and Emergency Alerts. Emergency Alert tones are configured under **Additional Features → Emergency Alerts**.

| | |
|---|---|
| Ring/Alert Tone | Select an audio file to play when a ring event is detected on the SIP Ring Extension. Test the audio file using the Play, Loop, and Stop buttons.<br><br>During multicast, the device will broadcast an audio stream using the Transmitter's selected ringtone. This is the default tone that will be played if selected in the settings **Multicast → Additional Ring Extension**. |
| Ring/Alert Volume | Set the volume for a SIP Ring event using the dropdown. |

| | |
|---|---|
| | This setting is for gain control and the output level depends on the levels recorded into the source audio file played from memory. This setting is only used for local tones, not multicast.<br><br>See Page Speaker Volume below for the volume settings used for all audio received over multicast. |
| Ring Limit | Typically set to no limit. Ring Limit will limit how long the speaker will ring before timing out. A new ring event must occur for the speaker to play the audio file again. |

| **Inbound Page Settings** | |
|---|---|
| Page Speaker Volume | This setting is for gain control for SIP or multicast paging. The output level will depend on the streaming level. Page Speaker Volume will apply to all inbound multicast streams (for Receiver mode only) regardless of audio source or type. |
| Page Mode | Set calls to the SIP page extension as one-way, two-way, or delayed.<br><br>In delayed mode, the speaker will record a message to be played after hanging up. The device will buffer an announcement up to 5 minutes long.<br><br>To cancel a page while in delayed mode, press “*” while recording to prevent it from being sent after hanging up. |
| Page Timeout | Set the maximum duration for a page. The page will end when the timeout limit has been reached. This is useful to ensure the paging system is not stuck in an active state in cases where someone accidentally forgets to hang up or puts the call on hold by mistake. |
| Page Tone | Select a pre-page tone to be played when a page is starting. Use only the Default or custom uploaded files. |

| | |
|---|---|
| | Other pre-installed tone files contain silence at the end to generate a ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a page. The "Default" tone is set to page-notif.wav.<br>The **Default Page Tone** in **Advanced Multicast** will play the tone set here. |
| G.722 Support | Enable or disable the G.722 codec. G.722 enables wideband audio for optimum speech intelligibility. |
| Passcode Protected Page Extensions | When enabled, the caller must enter the set passcode followed by the # sign before the page can be made. Setting a passcode helps prevent unintentional pages. |
| Apply to All Page Extensions | Only visible when **Passcode Protected Page Extensions** is set to **Enabled**. Enable or disable a passcode for all page extensions. |
| Passcode | Only visible when **Passcode Protected Page Extensions** is set to **Enabled**. Passcodes can be up to 15 digits and must be numbers only. |
| Passcode Prompt Tone | Only visible when **Passcode Protected Page Extensions** is set to **Enabled**. Select the tone to be played to prompt the user to enter the passcode before paging. |
| DTMF Detection Type | Select the preferred dual-tone multi-frequency (DTMF) detection method. DTMF is a technology used with touch tone phones (the sound made when pressing a number key). The 8190 uses this for multi-zone selection, passcode, etc. |

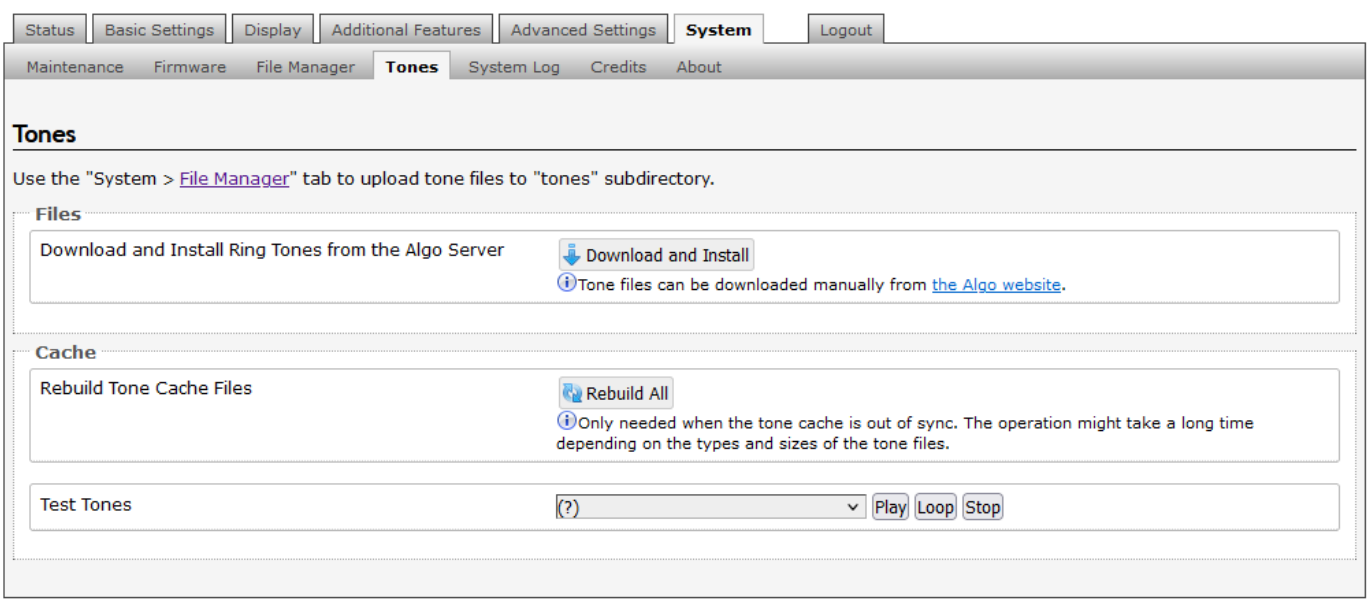
| **Outbound Page Settings** | |
|---|---|
| Outbound Ring Limit | Typically set to ensure that a call will not reach voicemail. This feature can be used to set a limit on how long the speaker will ring before timing out. |
| Ringback Tone | Allow audible ringback tone to be played over the speaker until the call is answered. |

| | |
|---|---|
| Allow Call Button to End Active Call | Select an action to occur if the call button is pressed while a call is active. A secondary action can be disabled, set to end the call, or end the call and redial. |

| **Audio Processing** | |
|---|---|
| Ambient Noise Compensation | When enabled, Ambient Noise Compensation will allow the speaker level to adjust automatically in response to ambient noise levels detected at the device before the start of each call. The volume is adjusted automatically via the speaker's microphone. |
| Automatic Gain Control (AGC) | Enable or disable AGC to normalize the audio level. Enabling ensures the speaker is always played at a consistent volume. |

# Tones

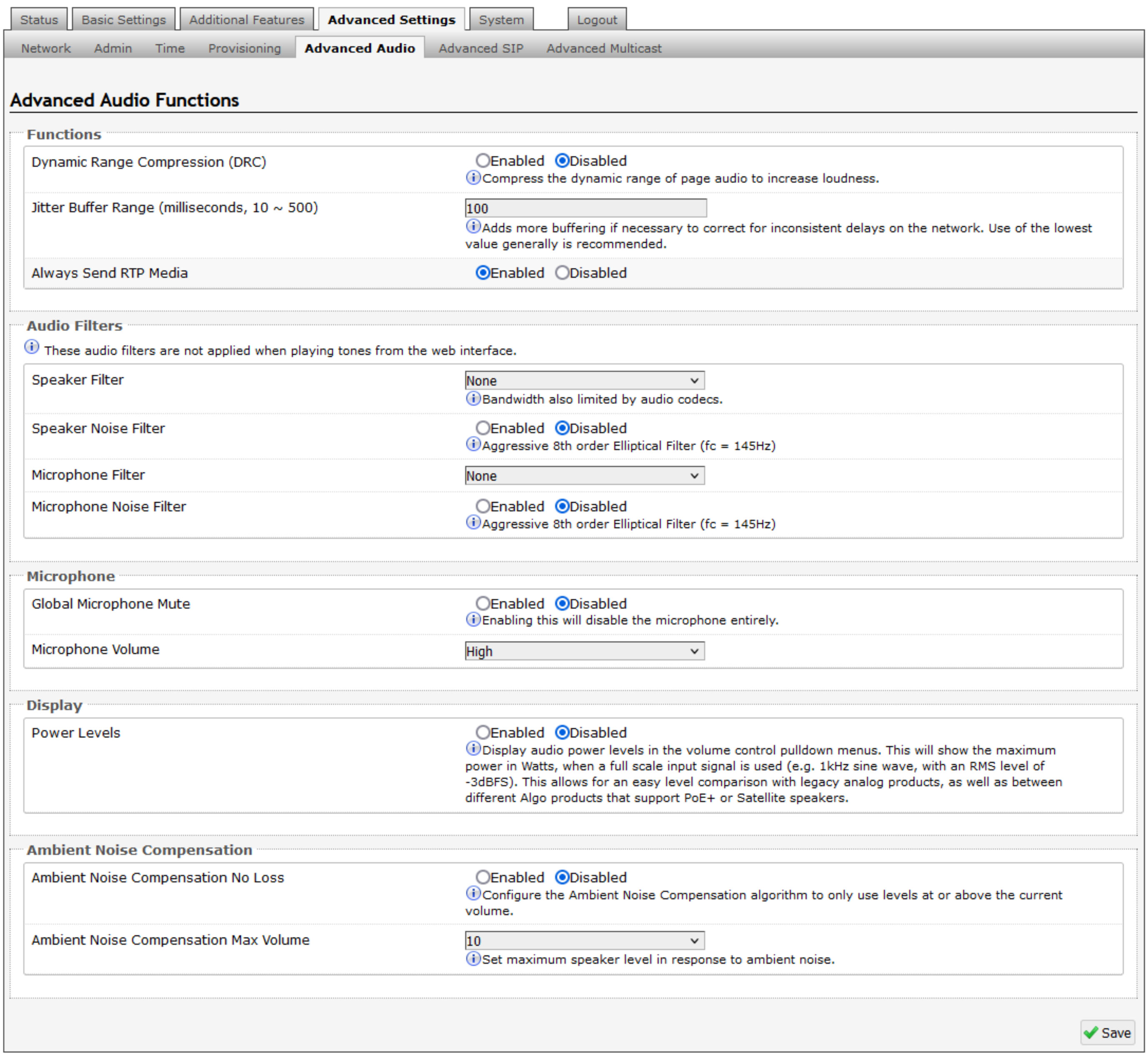
The 8190 includes several pre-loaded audio files that can be selected to play for various events. The web interface allows you to select a file and play it immediately over the speaker for testing, available in **Basic Settings** → **Features**. Files may also be added, deleted, or renamed. For more information see File Manager.




| **Files** | |
|---|---|
| Download and Install Ring Tones from the Algo Server | Tone files can be downloaded manually from the Algo website. |

| Cache | |
|---|---|
| Rebuild Tone Cache Files | Only needed when the tone cache is out of sync. The operation might take a long time depending on the types and sizes of the tone files. |
| Test Tones | Listen to uploaded audio files via the device. |

# Advanced Audio




| Functions |
|---|

| | |
|---|---|
| Dynamic Range Compression (DRC) | Enable to compress the dynamic range of page audio to increase loudness. |
| Dynamic Range Compression Gain | Select the amount of compression gain from the dropdown menu. More gain increases distortion. |
| Jitter Buffer Range | Enter a value between 10-500 to add more buffering if necessary to correct for inconsistent delays on the network. It is recommended to use the lowest value. |
| Always Send RTP Media | Enable to send audio packets at all times, even during one-way paging mode. This option is needed when the server expects to always see audio packets. |

| **Audio Filters** | |
|---|---|
| Speaker Filter | Select a frequency from the dropdown to apply a high-pass filter to the speaker output. This setting reduces audio artifacts like humming or buzzing by filtering out unwanted frequencies. |
| Speaker Noise Filter | Enable to filter below 145 Hz to reduce mains-induced noise like fans. |
| Microphone Filter | Select a frequency from the dropdown to apply a high-pass filter to the microphone input. This setting reduces audio artifacts like humming or buzzing by filtering out unwanted frequencies. |
| Microphone Noise Filter | Enable to filter below 145 Hz to reduce mains-induced noise like fans. |
| Speaker Array Directionality Control | The 8190 uses a multi-speaker line array for improved sound distribution. Enable to control dispersion in the vertical axis reduces reflections from the floor and ceiling for more consistent direct sound levels for listeners at different distances from the speaker. |

| **Microphone** | |
|---|---|
| Global Microphone Mute | Enable to disable the microphone entirely. |

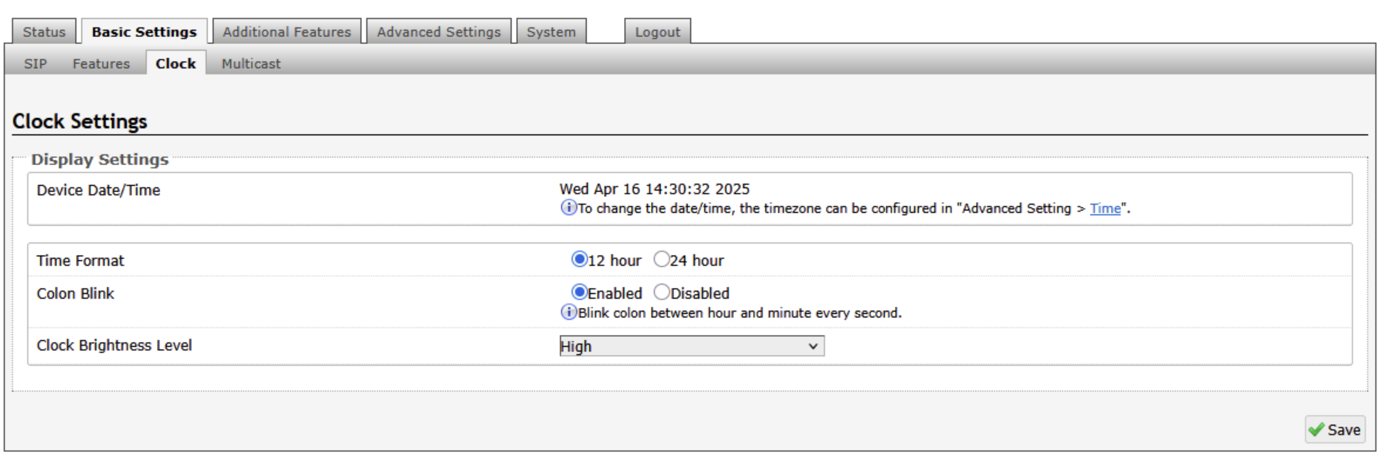
| | |
|---|---|
| Microphone Volume | Select a volume for the microphone. |

| **Display** | |
|---|---|
| Power Levels | Enable to display audio power levels in the volume control pulldown menus. This will show the maximum power in Watts when a full scale input signal is used (e.g. 1kHz sine wave, with an RMS level of -3dBFS). This allows for an easy level comparison with legacy analog products or other Algo products that support PoE+ or satellite speakers. |

| **Ambient Noise Compensation**<br>Only available if **Ambient Noise Compensation** is **Enabled** in **Basic Settings** → **Features**. | |
|---|---|
| Ambient Noise Compensation No Loss | Configure the Ambient Noise Compensation algorithm to only use levels at or above the current volume. The current volume is the minimum volume when this setting is enabled. |
| Ambient Noise Compensation Max Volume | Based on ambient noise levels, a maximum volume can be set. |

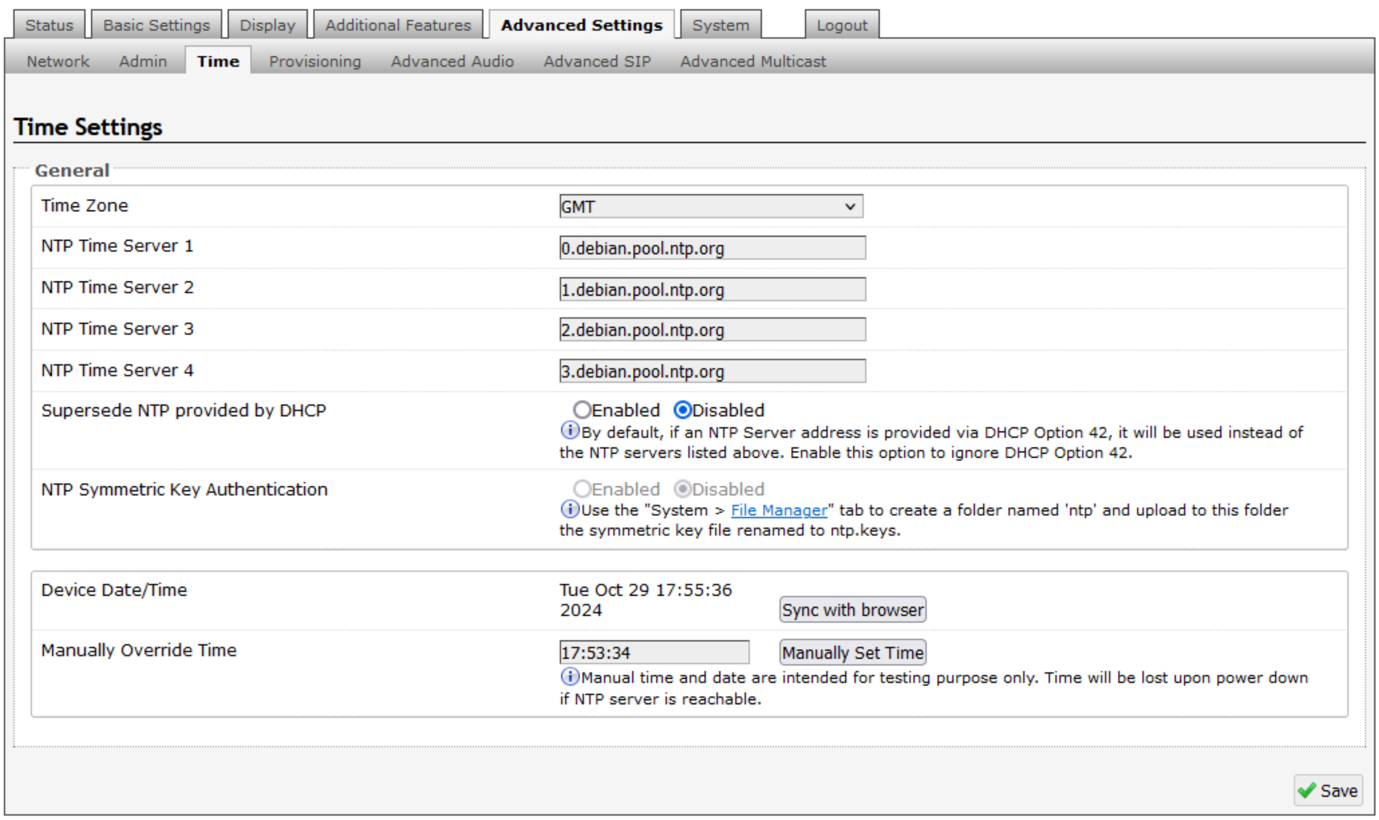
# Clock Configuration

## Basic Clock Settings



| **Display Settings** | |
|---|---|
| Device Date/Time | View the set time for the device. The timezone can be reconfigured in Advanced Settings → Time. |
| Time Format | Set the clock to display in **12 hour** or **24 hour** format. |
| Colon Blink | Enable or disable the colon blinking every second. |
| Clock Brightness Level | Set the clock brightness to Off, Low, Medium, or High. |

# Time




| **Time Settings** | |
|---|---|
| Time Zone | Use the dropdown to select the time zone required for your device. |
| NTP Time Server | The interface will attempt to use Timer Server 1 and work down the list if one or more of the time servers become unresponsive.<br>These settings are pre-populated with public NTP servers |

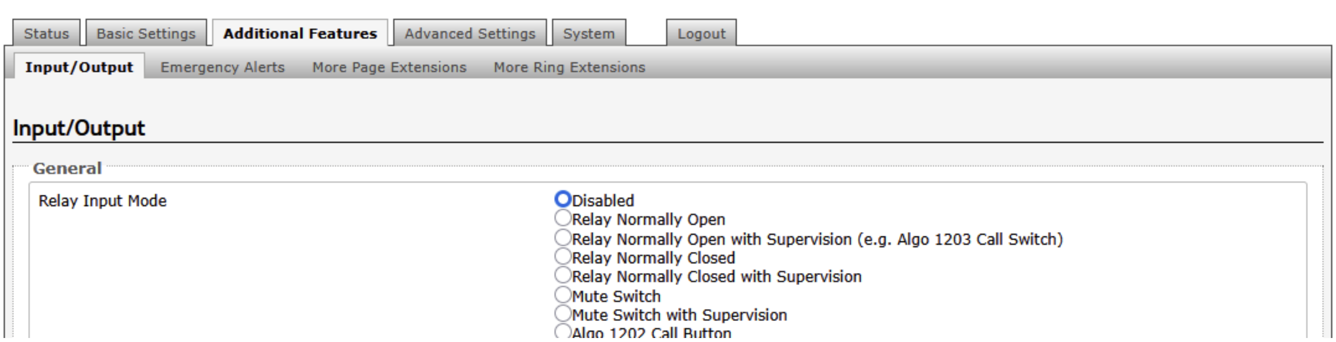
| | |
|---|---|
| | hosted on the internet. To use these, the device requires internet connection. Alternatively, this can be customized to point the device to any other NTP server hosted or premise-based. |
| Supersede NTP provided by DHCP | By default, if an NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed above. Enable this option to ignore DHCP Option 42. |
| NTP Symmetric Key Authentication | To enable, create a new folder in the tab **System → File Manager** and create a folder named *ntp.* Upload the symmetric key file and rename the file to *ntp.keys*. |
| Device Date/Time | This field shows the current time and date set on the device. If you are testing the device on a lab network that does not have access to an external NTP server, click Sync with browser to temporarily set the time on the device.<br>This time value will be lost at power down or overwritten if connection to the NTP server is available. Time and date are used for logging purposes. |
| Manually Override Time | Manual time and date are intended for testing purposes only. Time will be lost upon power down if the NTP server is reachable. |

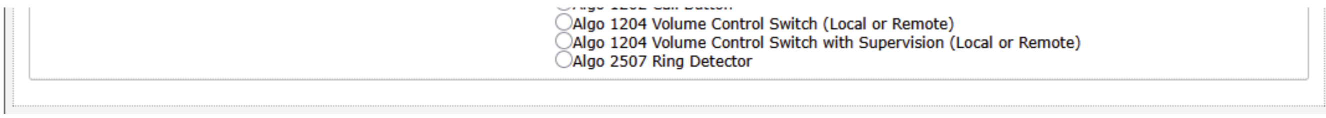
---

# Relay Input/Output Configuration

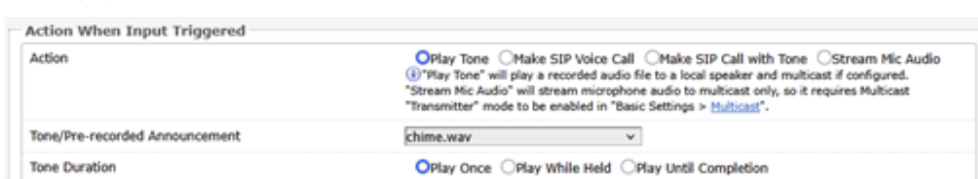
The 8190 has dry contact input and output terminals to connect external accessories, including Algo and third-party accessories.

**General**





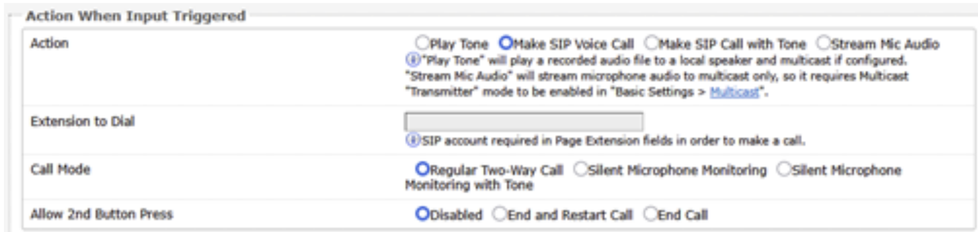

| | |
|---|---|
| Relay Input Mode | Options for Relay Input Mode include:<br>• Disabled<br>• Relay Normally Open<br>• Relay Normally Open with Supervision (e.g. Algo 1203 Call Switch)<br>• Relay Normally Closed<br>• Relay Normally Closed with Supervision<br>• Mute Switch<br>• Mute Switch with Supervision<br>• Algo 1202 Call Button<br>• Algo 1204 Volume Control Switch (Local or Remote)<br>• Algo 1204 Volume Control Switch with Supervision (Local or Remote)<br>• Algo 2507 Ring Detector<br>Notification actions can be triggered via supervision settings if the input switch is disconnected.<br><br>For more information on how to configure each of these devices with the 8190, see Wiring Connections. |

| **Action When Input Triggered** | |
|---|---|
| Action | **Play Tone**<br>When the 8190 input is triggered, a tone or a pre-recorded audio file will play over the speaker or multicast. This function can be used to request support or assistance in service or retail environments, notify about an emergency at a specific location in medical or educational facilities, or sound an alarm during an intrusion.<br> |

<table>
<tr><td></td><td>

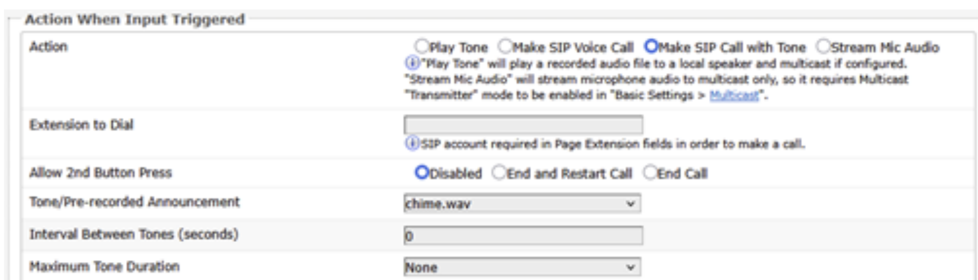
**Mak SIP Voice Call**

When the 8190 input is triggered, a voice path will open for an intercom-like call. This option can be used when a call needs to be made from a public place where a telephone would not be practical to use.




**Make SIP Call with Tone**

When the 8190 input is triggered, a private call can be made to a pre-configured telephone extension with a pre-recorded message. For instance, a call to a supervisor’s telephone notifying about an emergency or intrusion at some location.




**Stream Mic Audio**

Will stream microphone audio to multicast only. Requires multicast “Transmitter” mode to be enabled.

</td></tr>
<tr><td>Tone/Pre-recorded Announcement</td><td>Available when Action is set to Play Tone or Make SIP Call with Tone.<br><br>Select a recording or tone to use. Custom audio files may be used and uploaded through System → File Manager.</td></tr>
<tr><td>Tone Duration</td><td>Available when Action is set to Play Tone.</td></tr>
<tr><td>Extension to Dial</td><td>Available when Action is set to Make SIP Voice Call or Make SIP Call with Tone.<br><br>A SIP account is required in Page Extension fields to make a call.</td></tr>
<tr><td>Call Mode</td><td>Available when Action is set to Make SIP Voice Call.</td></tr>
</table>

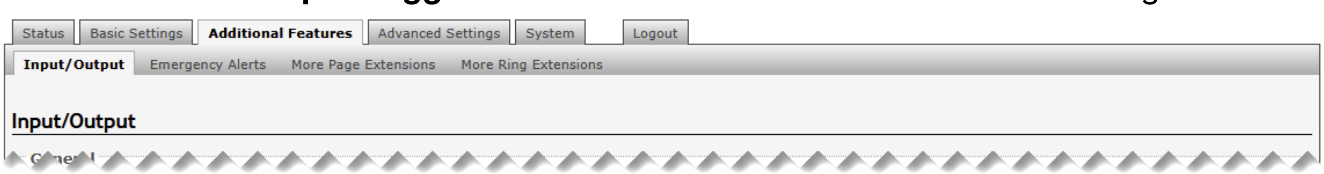
| | |
|---|---|
| Allow 2nd Button Press | Available when **Action** is set to **Make SIP Voice Call** or **Make SIP Call with Tone**.<br><br>If enabled, the 2nd button press will End Call or End and Restart Call. Therefore, if an input is triggered a second time, the SIP call will be terminated and, in some cases, immediately called again. |
| Interval Between Tones | Available when **Action** is set to **Make SIP Call with Tone**.<br><br>Specify the time delay (seconds) between tones. |
| Maximum Tone Duration | Available when **Action** is set to **Make SIP Call with Tone**.<br><br>Select the maximum tone duration. The tone will be terminated once the maximum time is reached. |

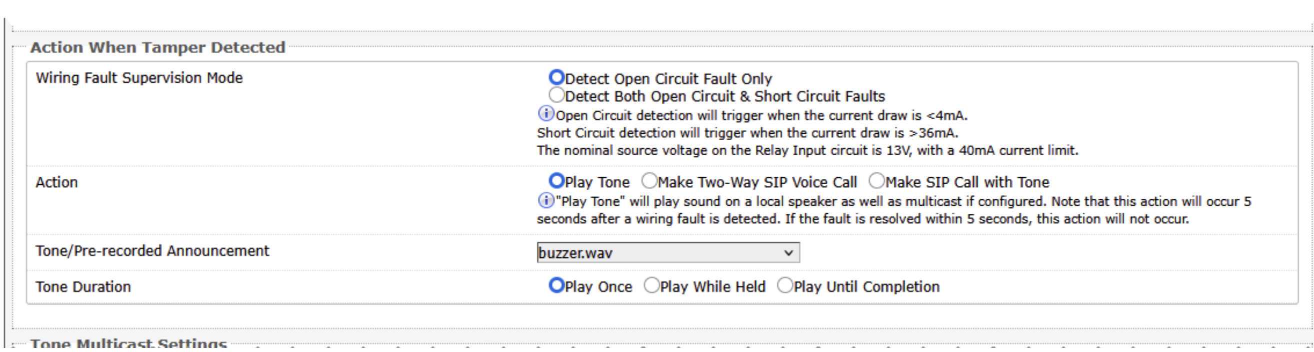
**Action When Tamper Detected**

The 8190 can be configured with supervision to execute one of the above three actions (**Play Tone**, **Make SIP Voice Call**, **Make SIP Call with Tone**) if the accessory device connected to the relay input goes offline due to a wiring failure or after being tampered with.

For example, a tone could sound over the speaker(s) or a private pre-recorded message could be sent to a specified telephone extension. The supervision configuration options will appear if a Relay Input Mode with supervision is selected.

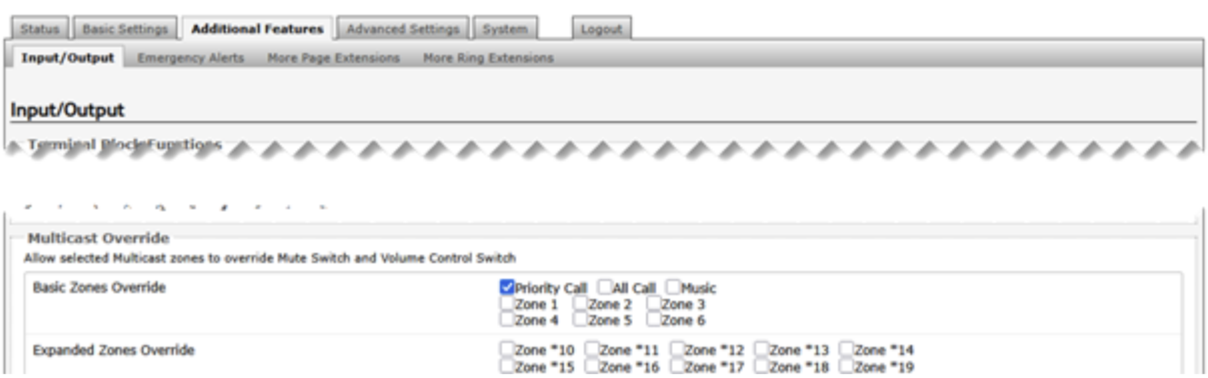
See **Action When Input Triggered** above for information on additional settings.

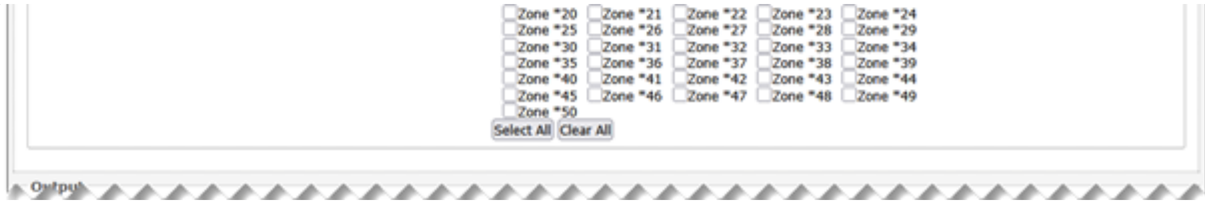


| | |
|---|---|
| Wiring Fault Supervision Mode | Open circuit detection will be triggered when the current draw is <4 mA. Short circuit detection will trigger when the current draw is →36 mA. The nominal source voltage on the Relay Input circuit is 13 V with a 40 mA current limit. |
| Action | **Play Tone**<br>When the 8190 input is triggered, a tone or a pre-recorded audio file will play over the speaker or multicast. For example, an audio file with the announcement: "Wiring fault detected on the emergency button of the Algo 8190 in the warehouse."<br><br>**Make SIP Voice Call**<br>When the 8190 input is triggered, a voice path will open for an intercom-like call.<br><br>**Make SIP Call with Tone**<br>When the 8190 input is triggered, a call can be made using a pre-recorded audio file describing the failure. |
| Tone/Pre-recorded Announcement | Available when **Action** is set to **Play Tone** or **Make SIP Call with Tone**.<br><br>Select a recording or tone to use. Custom audio files may be used and uploaded through **System → File Manager**. |
| Tone Duration | Available when **Action** is set to **Play Tone**. |

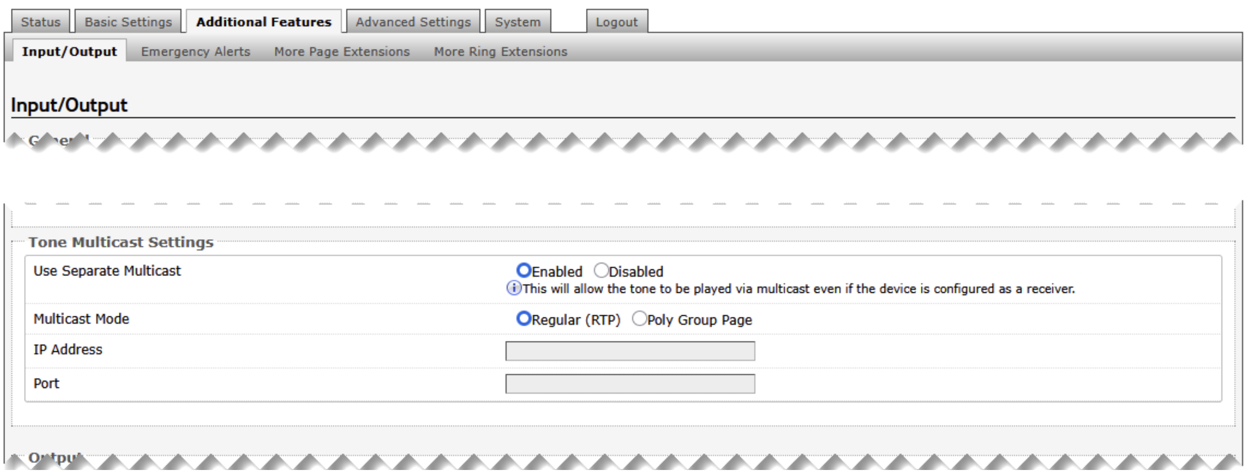
**Multicast Override**





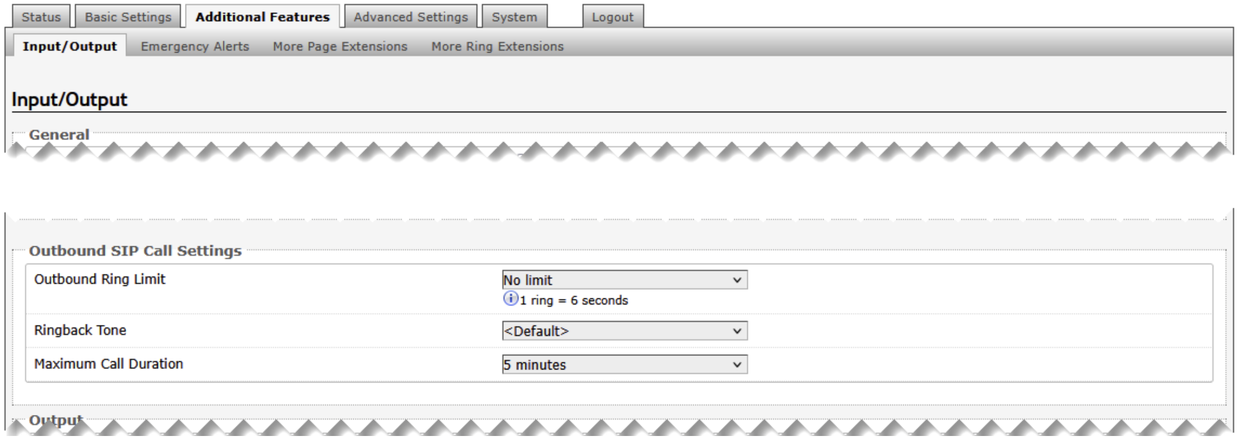

| | |
|---|---|
| Basic Zones Override | Select basic zones to give multicast priority to and override the volume set by the Volume Control Switch. |
| Expanded Zones Override | Select expanded zones to give multicast priority to and override the volume set by the Volume Control Switch. |

## Tone Multicast Settings




| | |
|---|---|
| Use Separate Multicast | When enabled, the set tone will be played via multicast even if the 8190 is configured as a receiver. To do this, a different multicast channel must be used to transmit audio. The separate multicast address must use a different port number from any of the zones that are already used as listening zones. |
| Multicast Mode | Use the same details as the receiver zone that is being listened to. |
| IP Address | Use the same details as the receiver zone that is being listened to. |
| Port | Use the same details as the receiver zone that is being listened to. |

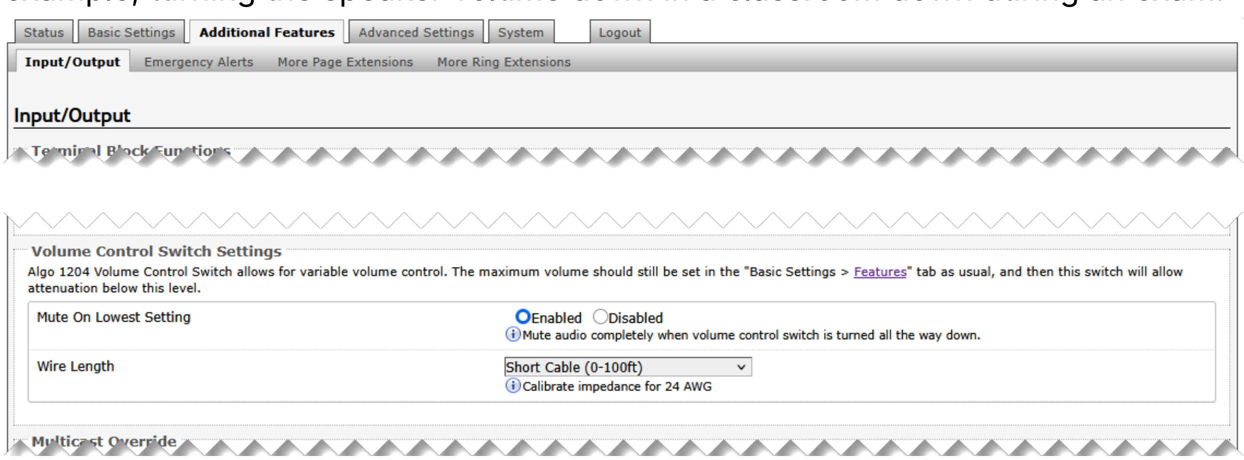
## Outbound SIP Call Settings




| | |
|---|---|
| Outbound Ring Limit | Available when **Action** is set to **Make SIP Voice Call** or **Make SIP Call with Tone**.<br>Select the number of rings that will occur before the call reaches voicemail. One ring is six seconds. |
| Ringback Tone | Available when **Action** is set to **Make SIP Voice Call**.<br>Select a ringback tone to play during an outbound SIP call while waiting for the far-end party to answer. |
| Maximum Call Duration | Available when **Action** is set to **Make SIP Voice Call**. |

## Volume Control Switch Settings

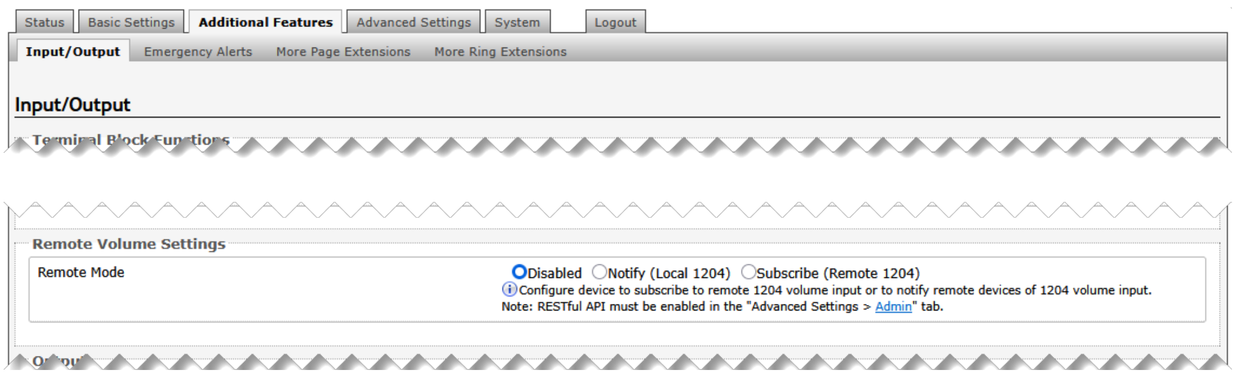
Available when the Algo 1204 Volume Control Switch is selected as the relay input device. The settings below allow for variable volume control in the speaker location. For example, turning the speaker volume down in a classroom down during an exam.



| | |
|---|---|
| Mute on Lowest Setting | Enable to mute audio when the volume control switch is turned to the lowest setting (1) |
| Wire Length | Set to calibrate impedance for 24 AWG. |

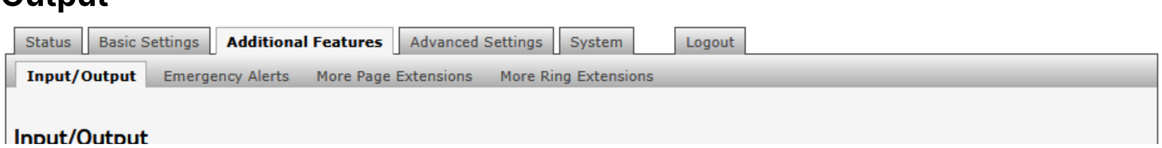
**Remote Volume Settings**

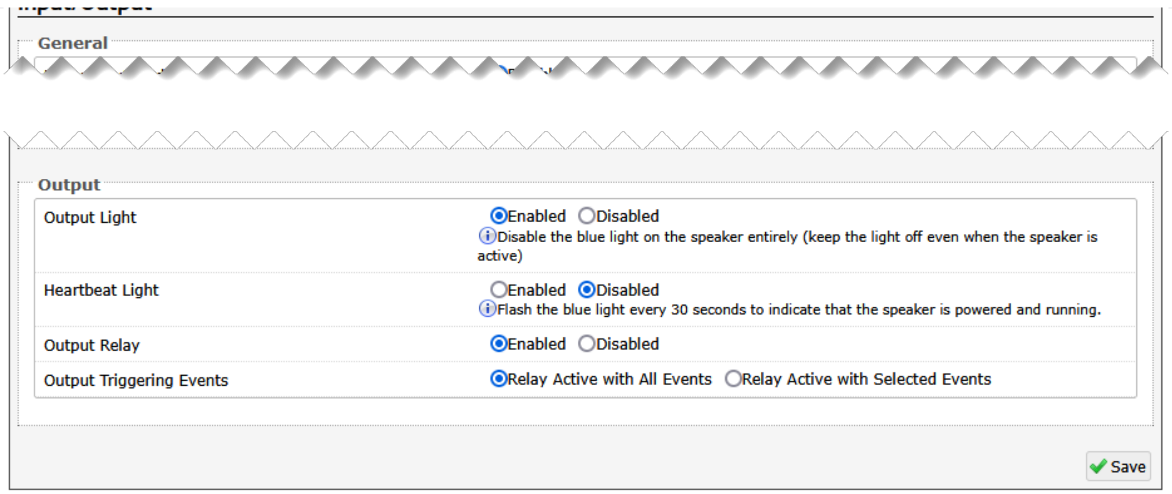
Available when the Algo 1204 Volume Control Switch is selected as the relay input device. This feature allows one 1204 to change the volume on multiple speakers. For example, changing the volume of multiple speakers in a school theatre.




| | |
|---|---|
| Remote Mode | Configure the device to subscribe to a remote 1204 volume input or to notify remote devices of 1204 volume input.<br><br>Note that if Notify (Local 1204) or Subscribe (Remote 1204) are selected, the RESTful API must be enabled under **Advanced Settings** → **Admin**. |
| IP Address | Only used if **Remote Mode** is set to **Subscribe (Remote 1204)**. The IP address of the Algo IP endpoint with a connected 1204. |
| Remote Device RESTful API Password | The RESTful API password used between the two (or more) Algo devices that are sharing a single 1204. The password must be the same across all devices. |

**Output**

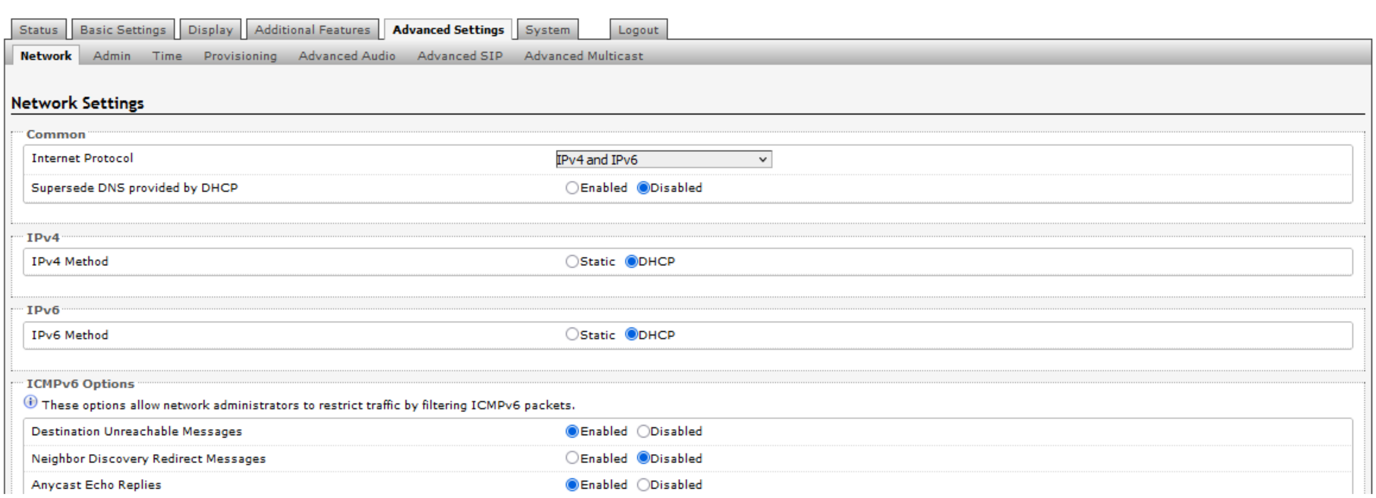


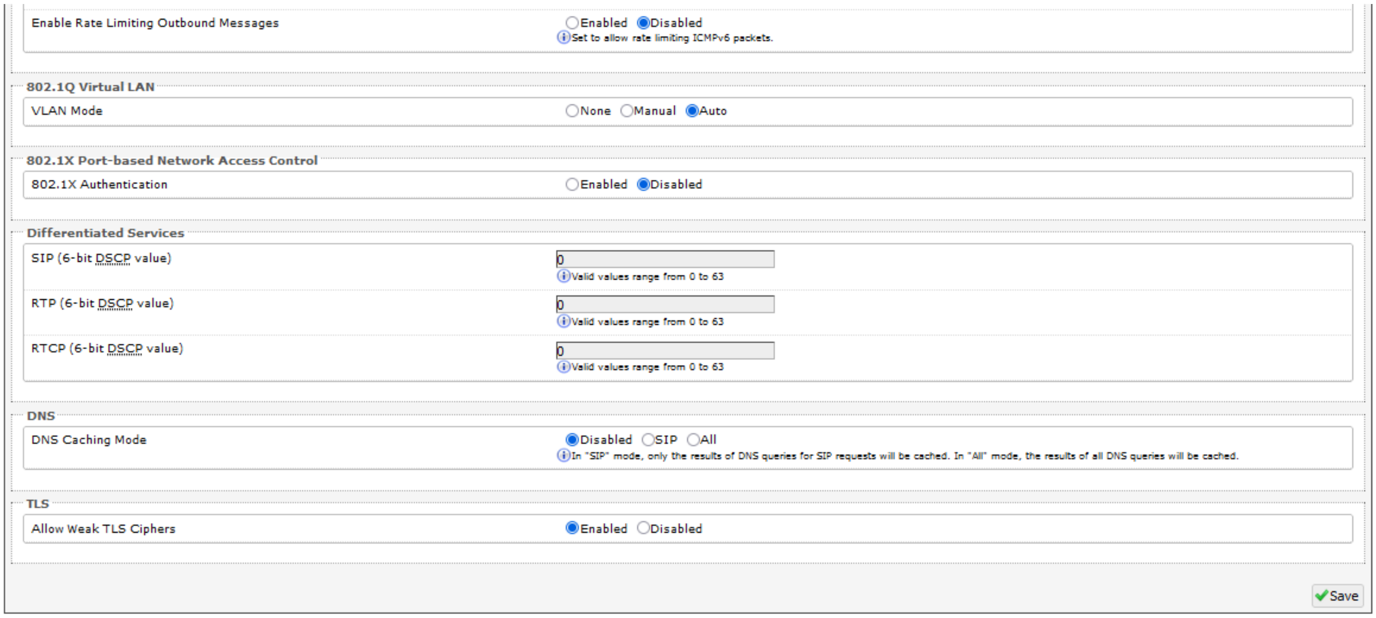



| | |
|---|---|
| Output Light | Enable or disable the blue light on the speaker entirely (keep the light off even when the speaker is active). |
| Heartbeat Light | Enable to flash the blue light every 30 seconds to indicate that the speaker is powered and running. |
| Output Relay | This setting controls whether the output relay activates or not. Note that when enabled, the output relay will activate whenever the 8190 is activated (paging, alerting, etc.) This is a normally open relay only. |
| Output Triggering Events | Select an event to trigger the output relay. |

# System Configuration

## Network Settings






| **Common** | |
|---|---|
| Internet Protocol | Use the dropdown to select **IPv4 Only** or **IPv4 and IPv6**. |
| Supersede DNS provided by DHCP | This setting will not appear if the selected Internet Protocol is set to **Static**. When enabled, this configuration allows DNS settings to be manually configured, replacing ones that may have been provided via DHCP. |

| **IPv4** | |
|---|---|
| IPv4 Method | The device can be set to a static or DHCP IP address.<br><br>DHCP is an IP standard designed to simplify the administration of IP addresses. When selected, DHCP will automatically configure IP addresses for each device on the network. DHCP is selected by default.<br><br>When Static is selected, the device will use the IP address entered in the fields below. |
| IPv4 Address/Netmask | Enter the static IP address and netmask (CIDR format) for the device (e.g., 192.168.1.23/24 where "/24" is equivalent to a netmask of 255.255.255.0). |
| IPv4 Gateway | Enter the gateway address. |

| IPv6 | |
|---|---|
| IPv6 Method | The device can be set to a static or DHCP IP address.<br><br>DHCP is an IP standard designed to simplify the administration of IP addresses. When selected, DHCP will automatically configure IP addresses for each device on the network.<br><br>When Static is selected, the device will use the IP address entered in the fields below. |
| IPv6 Address/Netmask | Enter the static IP address and netmask (CIDR format) for the device (e.g., 2001:123::abcd:1234/64). |
| IPv6 Gateway | Enter the gateway address. |

| ICMPv6 Options | |
|---|---|
| Destination Unreachable Messages | Enable to restrict traffic by filtering ICMPv6 packets. |
| Neighbor Discovery Redirect Messages | Enable to restrict traffic by filtering ICMPv6 packets. |
| Anycast Echo Replies | Enable to restrict traffic by filtering ICMPv6 packets. |
| Enable Rate Limiting Outbound Messages | Enable to limit the device to respond to other network devices at the specified rate below and prevent it from receiving multiple requests at the same time. |
| Rate Limit (packets per second) | Specify the packets per second allowed for Rate Limiting Outbound Messages. |

| **802.1Q Virtual LAN**<br>If the device is using VLAN, you will need to be on the same VLAN to access the web interface, unless routing has been configured between VLANs. | |
|---|---|
| VLAN Mode | VLAN tagging is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and |

| | |
|---|---|
| | the accompanying procedures to be used by bridges and switches in handling such frames. The standard also provides provisions for a quality-of-service prioritization scheme known as IEEE 802.1p and defines the Generic Attribute Registration Protocol. |
| VLAN ID | Specify the VLAN that the Ethernet frame belongs to. The hexadecimal values 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs.<br><br>The reserved value 0x000 indicates that the frame does not belong to any VLAN. In this case, the 802.1Q tag specifies only a priority and is referred to as a priority tag. |
| VLAN Priority | Set the frame priority level. Otherwise known as Priority Code Point (PCP), VLAN Priority is a 3-bit field that refers to the IEEE 802.1p priority or frame priority level. Values are from 0 (lowest) to 7 (highest). |

| **802.1X Port-based Network Access Control** | |
|---|---|
| 802.1x Authentication | Enable to add credentials to access LAN or WLAN that have 802.1X network access control (NAC). You can ask your IT Administrator for this information |
| Authentication Mode | Select the desired authentication mode. |
| Anonymous ID | If configured, the device will send the anonymous ID to the authenticator instead of the 802.1X client username. |
| ID | The ID should contain a string identifying the IEEE 802.1X authenticator originating the request. Ask your IT administrator for details. |
| Password | Ask your IT administrator for details. |
| Validate Server Certificate | Enable to validate the authentication server against common authorities. To validate additional certificates, go to the System → File Manager to upload a Base64 encoded |

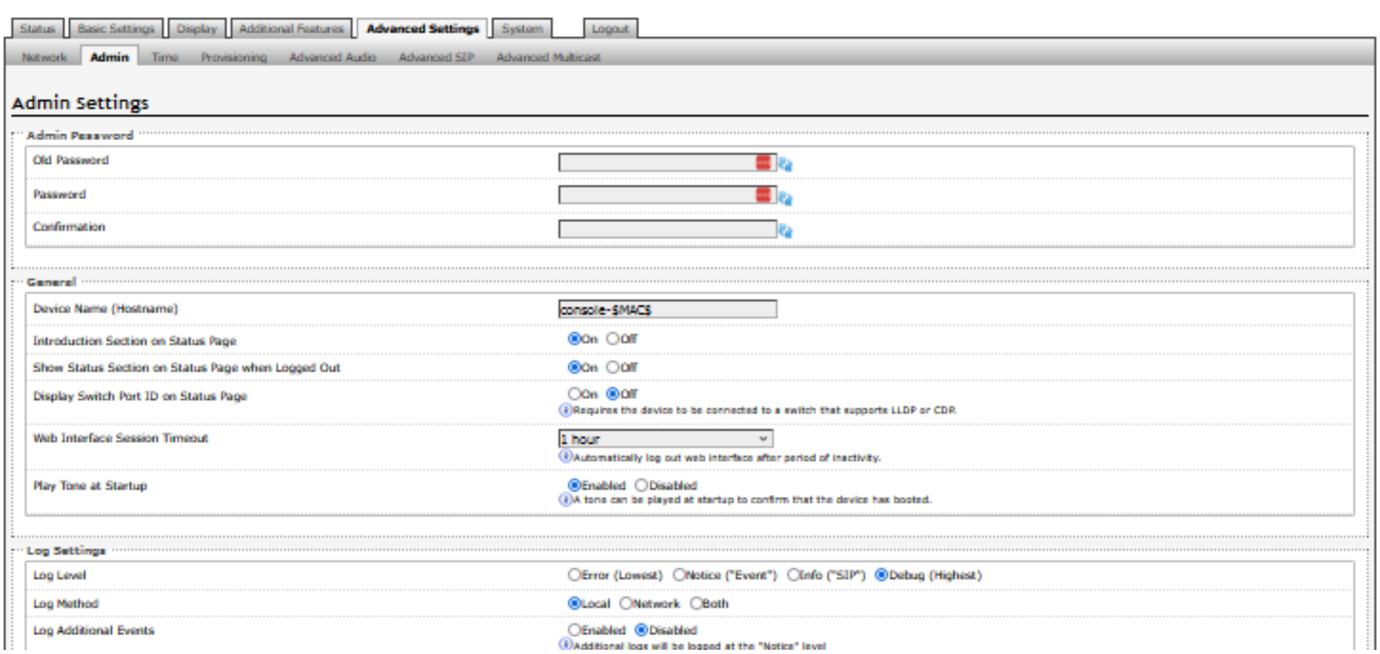
| | |
|---|---|
| | X.509 certificate file in .pem, .cer, or .crt format to the certs folder. |

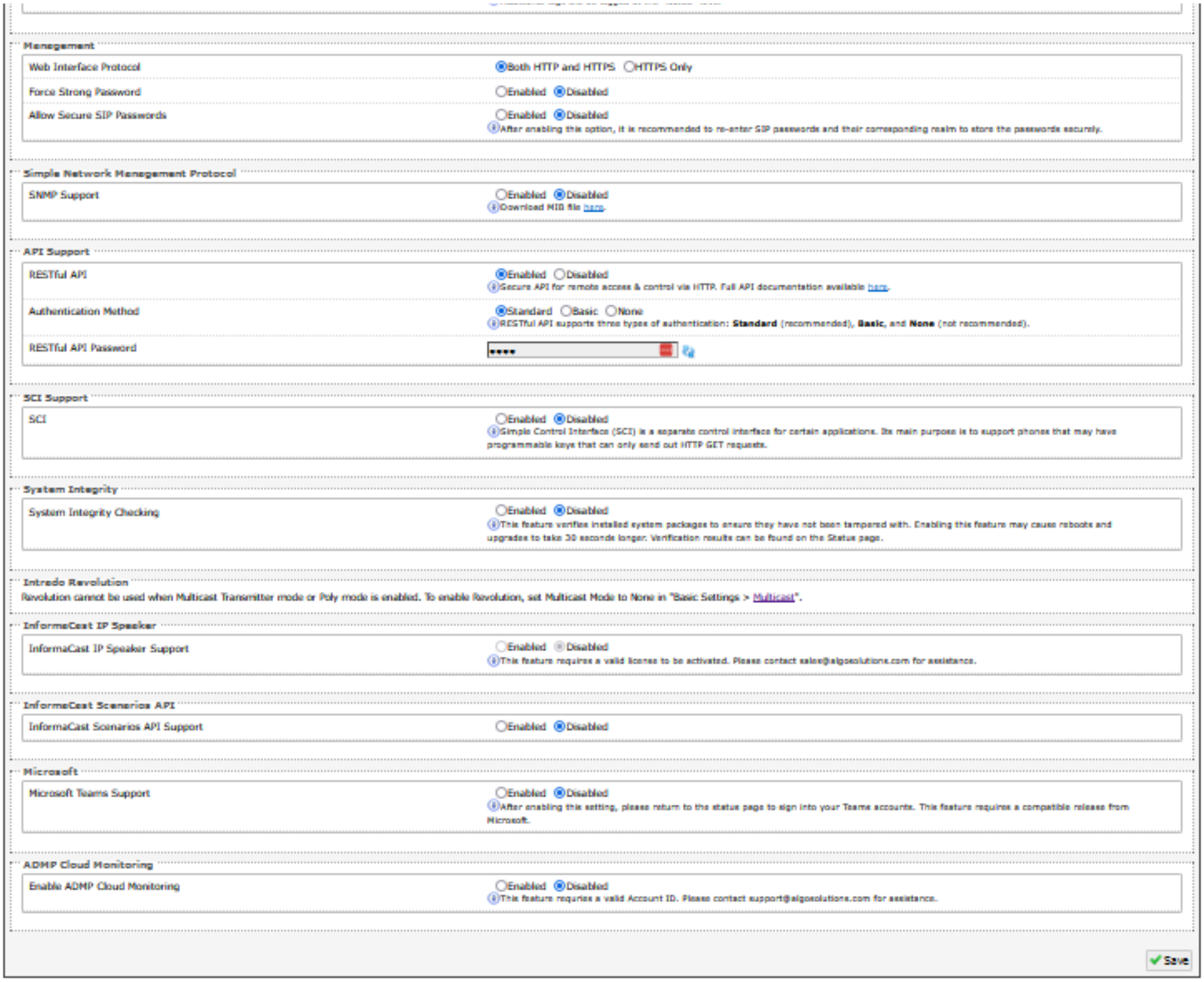
| **Differentiated Services** | |
|---|---|
| SIP (6-bit DSCP value) | Enter the DSCP value for SIP packets. |
| RTP (6-bit DSCP value) | Enter the DSCP value for RTP packets. |
| RTCP (6-bit DSCP value) | Enter the DSCP value for RTCP packets. |

| **DNS** | |
|---|---|
| DNS Caching Mode | There are three mode options:<br>1. **Disabled**: No DNS queries will be cached.<br>2. **SIP**: Only the results of DNS queries for SIP requests will be cached.<br>3. **All**: The results of all DNS queries will be cached |

| **TLS** | |
|---|---|
| Allow Weak TLS Ciphers | Enables compatibility with legacy systems that may not support the most current encryptions standards |

# Admin






| **Admin Password** | |
|---|---|
| Old Password | Enter the old admin password. The default password when you first get the device is algo. |
| Password | Enter a new admin password to log into the device web interface. Make sure the new password is stored safely. If the password is forgotten, you must reset the device entirely with the Reset Button to restore the default password. All other settings will be reset to the original default settings as well.<br><br>For additional password security, see the setting: Force Strong Password. |
| Confirmation | Re-enter your new admin password. |

| General | |
|---|---|
| Device Name (Hostname) | Add a name to identify the device in the Algo Network Device Locator Tool. |
| Introduction Section on Status Page | Turn On to show the introduction text on the login screen. |
| Show Status Section on Status Page when Logged Out | Turn On to allow others to view the status page without logging in. If turned Off, the settings and configurations on the status page will be hidden entirely unless a user is logged in to ensure only trusted users can view device information. |
| Display Switch Port ID on Status Page | Turn On to display the Switch Port ID on the Status Page. This option is only possible if the device is connected to a switch that supports LLDP or CDP. |
| Web Interface Session Timeout | Set the maximum duration of inactivity to log a user out of the web interface automatically. |
| Play Tone at Startup | The device can play a beep tone at startup. |

| Log Settings | |
|---|---|
| Log Level | This setting should only be used after consulting with the Algo support team. |
| Log Method | Select a Log Method:<br>• **Local**: The log file is saved in RAM on the device.<br>• **Network**: Send the log file to an external SysLog server so settings are not lost if the device is rebooted, or for ease of central access.<br>• **Both**: Use both methods. |
| Log Server | Enter the Syslog server address provided by your IT administrator. |
| Select Additional Log Events | To be used by support@algosolutions.com if necessary. |

| Management |
|---|

| | |
|---|---|
| Web Interface Protocol | HTTPS is always enabled on the device. HTTP is enabled by default but may be disabled. To do so, select HTTPS Only mode so requests are automatically redirected to HTTPS.<br><br>Note that no security certificate exists since the device can have any address on the local network. Therefore, most browsers will provide a warning when using HTTPS. |
| Force Strong Password | When Enabled, you can enforce a secure password for the device web interface for additional protection. The password requirements for a strong password are:<br>• Must contain at least 10 characters<br>• Must contain at least 1 uppercase character<br>• Must contain at least 1 digit (0 – 9)<br>• Must contain at least 1 special character |
| Allow Secure SIP Passwords | When **Enabled**, SIP passwords are stored in the configuration file in an encrypted format to prevent viewing and recovery. If enabled, navigate to **Basic Settings** → **SIP** and fill out the **Realm** field. To obtain your SIP Realm information, contact your SIP Server administrator or check the SIP log file for a registration attempt. The Realms may be the same or different for all the extensions used.<br><br>All the configured Authentication Password(s) must be re-entered here as well as any other locations where SIP extensions have been configured to save the encrypted password(s).<br><br>If the **Realm** is changed later, all passwords must be re-entered to save the passwords with the new encryption. |

| **Simple Network Management Protocol** | |
|---|---|
| SNMP Support | Disabled by default. The existing setting will respond to a simple status query for automated supervision. |

| | |
|---|---|
| SNMP Community String | Speak to your IT Administrator for more information. |
| SNMPv3 Security | Speak to your IT Administrator for more information. |

| **API Support** | |
|---|---|
| RESTful API | Disabled by default. Enable a secure API for remote access and device control via HTTP. For more information, see the Algo RESTful API Guide. |
| Authentication Method | Speak to your IT Administrator for more information. |
| RESTful API Password | Speak to your IT Administrator for more information. |

| **SCI Support** | |
|---|---|
| SCI | Disabled by default. Simple Control Interface (SCI) is a separate control interface for certain applications. Its primary purpose is to support phones that may have programmable keys that can only send out HTTP GET requests and allow them to initiate events remotely on an Algo device. |
| SCI Password | Enter your SCI password. |

| **System Integrity** | |
|---|---|
| System Integrity Checking | Enable this feature to verify that installed system packages have not been tampered with by running a check. Enabling this feature may cause reboots and upgrades to take 30 seconds longer. Verification results can be found on the Status tab. |

| **Power over Ethernet** | |
|---|---|
| PoE Power Detection | Use **Force PoE+** only when connected to a PoE+ power injector capable of providing 600mA that does not automatically negotiate its power capabilities. Incorrect use of this setting may cause the device to reboot if the power source is not |

| | |
|---|---|
| | capable of delivering the selected power. |

| **Intrado Revolution (formerly Syn-Apps)** | |
|---|---|
| Revolution Support | Enable the device to register with an Intrado Revolution Server and receive audio events from the system. |
| Revolution Server | Enter the Revolution Server to use the Revolution paging feature. Leave the field blank to use the server provided by the DHCP Option 72 |
| Local Management Port | Enter the local management port for the Revolution Server. |

| **InformaCast IP Speaker** | |
|---|---|
| InformaCast IP Speaker Support | This feature requires a valid InformaCast license to be activated. Please contact sales@algosolutions.com for assistance. |
| Configuration Mode | • **Auto**: The device will attempt to configure Informacast using DNS SRV, SLP, and/or via DHCP and TFTP<br>• **Manual:** The device will allow the configuration file location to be manually configured.<br>• **Direct:** The device will register to the list of static server addresses directly, bypassing the Configuration File Server |
| Configuration Retry Interval | Set the amount of time to wait before attempting to obtain configuration information after failure. |
| SIP Support | Enter the SIP credentials provided by InformaCast during configuration |
| Maximum Broadcast Duration | The maximum length of broadcast. |

| **InformaCast Scenarios API** | |
|---|---|
| InformaCast Scenario API Support | Enable the device to start an InformaCast Scenario via relay input. This feature can work without an InformaCast license, as only the output device requires a license. |

| Microsoft | |
|---|---|
| Microsoft Teams Support | Enable to allow the device to register with a Microsoft Teams account. The device reboot will take up to 5 minutes to complete, as the device will communicate several times with the Microsoft server. This feature requires a compatible release from Microsoft.<br><br>After enabling this setting, please return to the status page to sign into your Teams accounts. This feature requires a compatible release from Microsoft.<br><br>For more details, please see the Microsoft Teams Configuration Guide. |

| ADMP Cloud Monitoring | |
|---|---|
| Enable ADMP Cloud Monitoring | The Algo Device Management Platform (ADMP) simplifies the process of managing, monitoring, and maintaining Algo devices from any location. This feature requires a valid Account ID. To learn more about ADMP and how to purchase a license, visit the ADMP webpage. |
| Account ID | Enter the account ID listed on the Settings page of your ADMP account. |
| Allow Configuration File Sync | Enable ADMP to query and display settings stored on the device. |
| Heartbeat Interval | Select how often ADMP should check the status of your device. |

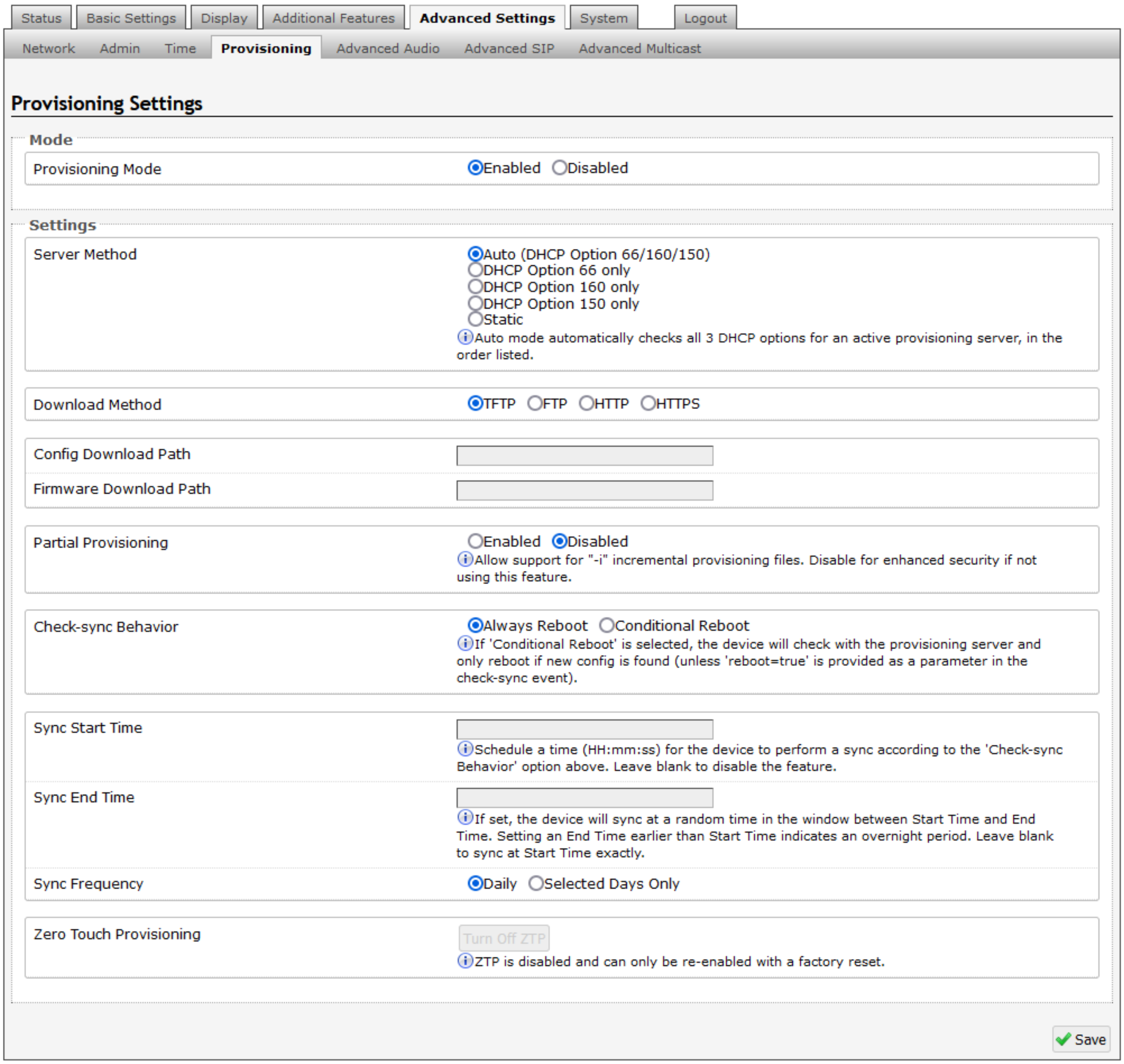
# Provisioning

Algo devices can be provisioned through a provisioning server or zero-touch provisioning (ZTP).

System administrators can provision multiple Algo devices together, eliminating the need to log into each endpoint web interface. After configuration or firmware files are placed on a provisioning server, Algo devices can be instructed to fetch these files and apply the settings.

Algo also offers a ZTP service that is meant to be used as a redirection service to your provisioning server or to configure your device with an Algo Device Management Platform (ADMP) account. ZTP is enabled by default and occurs before any other provisioning step. It will be disabled automatically after any other provisioning settings are changed on the device for the first time.

Visit the Algo Provisioning Guide for more information.




## Mode

| | |
|---|---|
| Provisioning Mode | Enabling provisioning allows installers to pre-configure the device on a network before installation. This is typically done for large deployments to save time and ensure consistent setups.<br><br>It is recommended that Provisioning Mode be set to Disabled if this feature is not in use. This will prevent unauthorized re-configuration of the device if DHCP is used. |

| **Settings** | |
|---|---|
| Server Method | Set to Auto by default. Select a Server Method.<br>• Auto: All three DHCP options (66, 160, 150) will be automatically checked for an active provisioning server<br>• DHCP Option 66 Only: Only DHCP Option 66 will be checked for a provisioning server<br>• DHCP Option 160 Only: Only DHCP Option 160 will be checked for a provisioning server<br>• DHCP Option 150 Only: Only DHCP Option 150 will be checked for a provisioning server<br>• Static: Only the specified static server will be checked for a provisioning server<br>For provisioning to work with a DHCP option, DHCP must be enabled under **Advanced Settings** → **Network** → **IPv4**. |
| Static Server | Enter the server address or domain. |
| Download Method | Select your preferred method for downloading provisioning files. The options are:<br>• TFTP (Trivial File Transfer Protocol) — See MD5 Checksum below for more details<br>• FTP<br>• HTTP<br>• HTTPS — This may help prevent configuration files from being read by an unwanted third party and having sensitive data stolen.<br>The device configuration files can be automatically downloaded |

| | |
|---|---|
| | from a provisioning server using DHCP Option 66. This option code (when set) supplies a TFTP boot server address to the DHCP client to boot from.<br><br>One of two files can be uploaded on the provisioning server (for access via TFTP, FTP, HTTP, or HTTPS):<br>• Generic (for all Algo 8190) algop8190.conf<br>• Specific (for a specific MAC address) algom[MAC].conf<br>Both protocol and path are supported for Option 66, allowing for http://myserver.com/config-path to be used. |
| Config Download Path | Enter the path where the configuration file is located in the provisioning server (e.g., algo/config/8190). |
| Firmware Download Path | Enter the path where the configuration file is located in the provisioning server (e.g., algo/config/8190). |
| Partial Provisioning | Enable to allow support for “-i” incremental provisioning files. Disable for enhanced security if this is not required. |
| Check-sync Behavior | Select Always Reboot to set the device to always reboot despite other settings.<br><br>Select Conditional Reboot to set the device and check the provisioning server. Only reboot if a new config is found (unless “reboot=true” is provided as a parameter in the check-sync event). |
| Sync Start Time | Set a time (HH:MM:SS) for the device to perform a sync according to the Check-sync Behavior setting. Leave this blank if not needed. |
| Sync End Time | If set, the device will sync randomly in the window between Sync Start Time and Sync End Time. Setting an End Time earlier than the Start Time indicates an overnight period. Leave blank to sync exactly at the set start time. |
| Sync Frequency | Select the sync frequency. Frequency can be set to Daily or Selected Days Only. |
| Sync Days | Select the days of the week for syncs to occur. |
| Zero Touch | ZTP is enabled by default but is disabled when any changes are |

| | |
|---|---|
| Provisioning | made to the device configuration. This button can also be used to disable ZTP if no changes have yet been made to the device configuration. |

## MD5 Checksum

If using TFTP as a download mode, a .md5 checksum file must be uploaded to the provisioning server In addition to the .conf file. This checksum file is used to verify that the .conf file is transferred correctly without error.

To generate a .md5 file, you can use tools such as http://www.fourmilab.ch/md5. To use this tool, simply download and unzip the .md5 program in a command prompt. The correct .md5 file will be generated in the same directory. To generate lowercase letters, use the “-l” parameter.

### Generating a generic configuration file

This configuration file is device-generic in terms of MAC address and will be used by all connected 8190 devices.

If using a generic configuration file, extensions and credentials must be entered manually once the 8190 has automatically downloaded the configuration file.

To see Algo’s SIP endpoint provisioning guide, visit www.algosolutions.com/provision

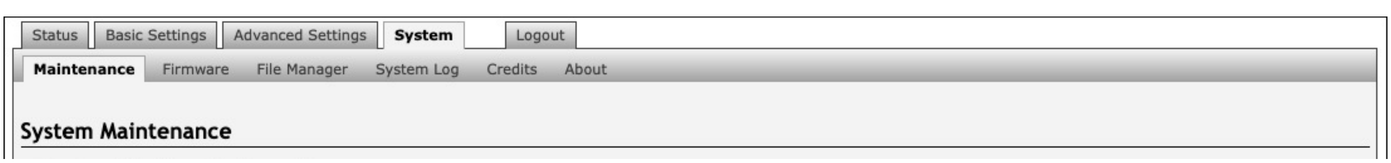
### Generating a specific configuration file

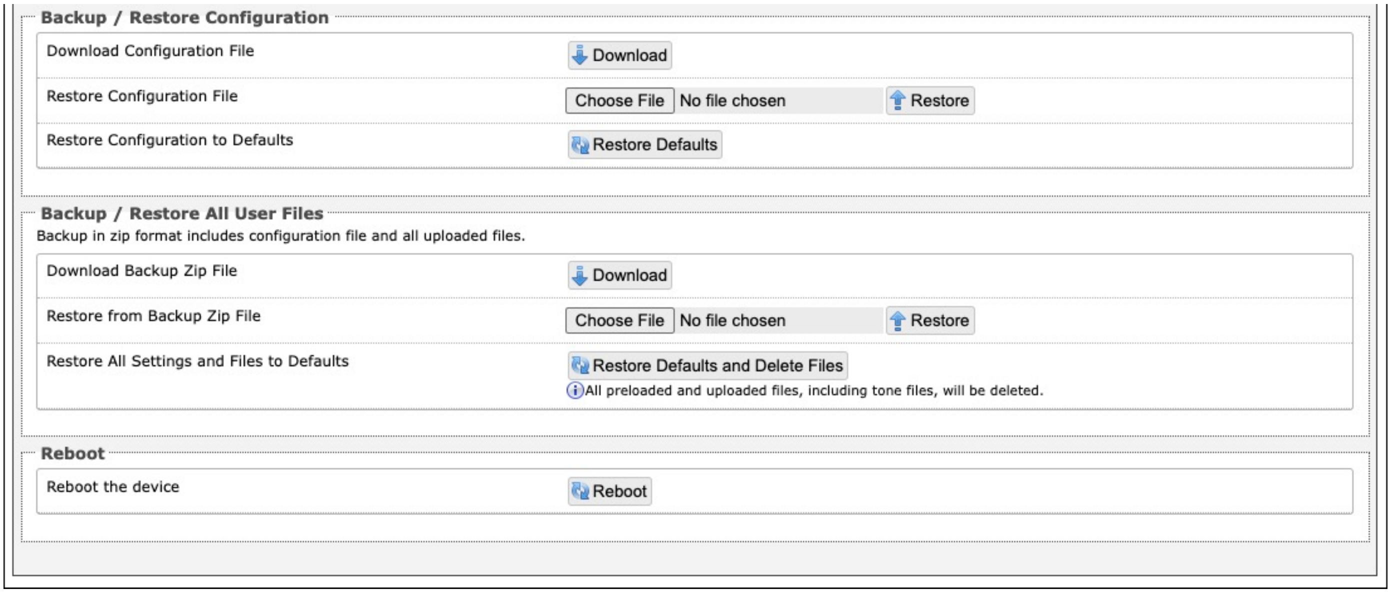
The specific configuration file will only be downloaded by the 8190 with the MAC address specified in the configuration file name.

Since all necessary settings can be included in this file, the 8190 will be ready to work immediately after downloading the configuration file. The MAC address of each 8190 can be found on the back label of the unit.

To see Algo’s SIP endpoint provisioning guide, visit www.algosolutions.com/provision

## System Maintenance



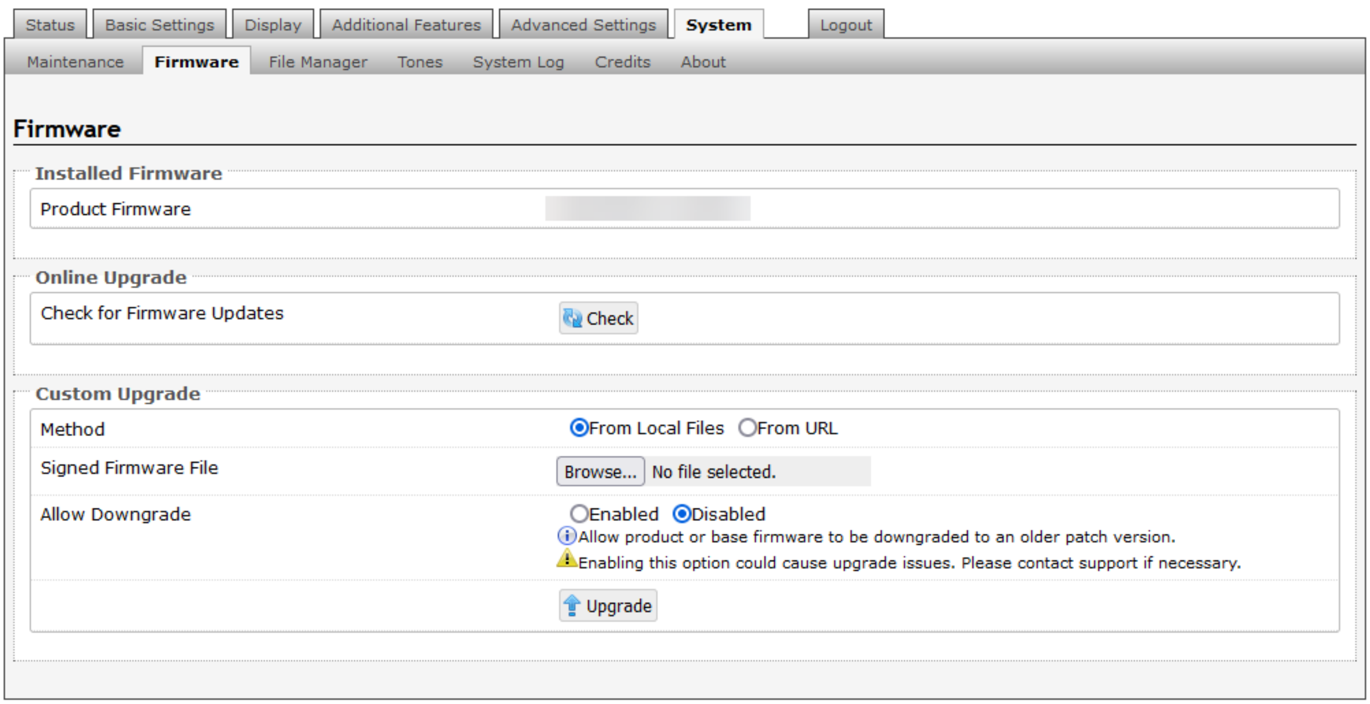



| **Backup/Restore Configuration** | |
|---|---|
| Download Configuration File | Save configuration settings to a text file for backup or to set up a provisioning configuration file. |
| Restore Configuration File | Restore settings by uploading a backup file. |
| Restore Configuration to Defaults | Reset all device settings to factory default values. |

| **Backup/Restore All User Files** | |
|---|---|
| Download Backup Zip File | Download the device configuration settings and the files in File Manager (ex., certificates, licenses, and tones) to a backup ZIP file. |
| Restore from Backup Zip File | Restore the device configuration settings and files in File Manager (ex., certificates, licenses, and tones) by uploading a backup zip file. |
| Restore All Settings and Files to Defaults | Reset the device configuration settings. All preloaded and uploaded files, including tone files, will be deleted. |

| **Reboot** | |
|---|---|
| Reboot the Device | Reboots the device. |

# Firmware




| **Installed Firmware** | |
|---|---|
| Product Firmware | Displays the current firmware on the device. |

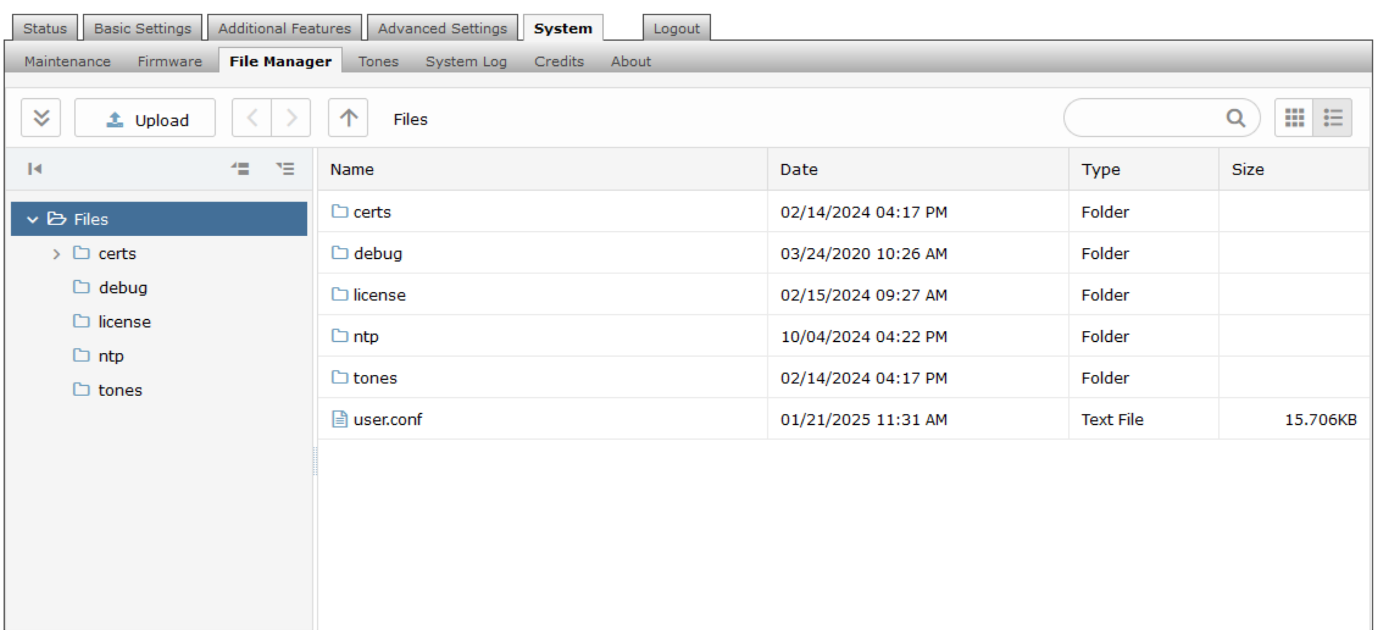
| **Online Upgrade** | |
|---|---|
| Check for Firmware Updates | Click **Check** to check for the latest firmware. If the firmware is up to date, Latest Firmware will state Firmware up to date. If your firmware is outdated, the new firmware availability will be listed. Internet connection is required. |

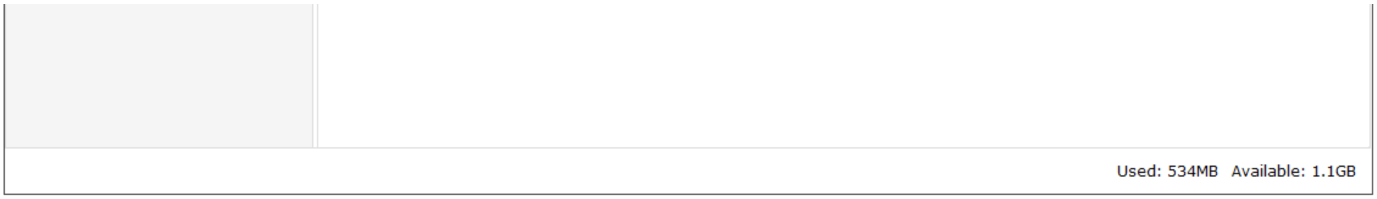
| **Custom Upgrade** | |
|---|---|
| Method | Select a method for firmware upgrades to occur. This can be done From Local Files or From URL. |
| Signed Firmware File | Use to upgrade firmware from a local file. To do this, download the firmware file from https://www.algosolutions.com/firmware-downloads/ then upload the file by clicking on Choose File and selecting the firmware file.<br><br>Click Upgrade at the bottom of the interface. |

| | |
|---|---|
| | Once the upgrade is complete, you can confirm the firmware version is changed by looking at the top right of the web interface. |
| Upgrade URL | Instead of downloading the firmware file https://www.algosolutions.com/firmware-downloads/, you may add the download link here instead.<br><br>Click Upgrade at the bottom of the interface.<br><br>Once the upgrade is complete, you can confirm the firmware version is changed by looking at the top right of the web interface. |
| Allow Downgrade | Enable to allow product to be downgraded to an older version. Enabling this option could cause future upgrade issues.<br><br>If you require downgrading, please contact support@algosolutions.com for assistance. |

# File Manager

The 8190 has 1 GB of storage space for additional files.






## certs Folder

If you have enabled **Validate Server Certificate** under **Advanced Settings** →**Advanced SIP** or **Advanced Settings** → **Provisioning** and want to validate against additional certificates, you can upload them here.

1. To install a public CA certificate on the Algo device, follow the steps below:
2. Obtain a public certificate from your Certificate Authority (Base64 encoded X.509 .pem, .cer, or .crt).
3. Open the **certs** folder in the web interface by going to **System** → **File Manager**.
4. Upload the certificate files into the **certs** folder by clicking Upload in the top left corner of the file manager and select the certificate.

Reach out to support@algosolutions.com to get the complete list of pre-loaded trusted certificates.

## debug Folder

If you have any challenges with the device and work with the Algo support team to overcome or fix them, the debug folder will be used. The device will generate files containing information about the device and put them in the debug folder. You do not need to use this folder unless directed to by the Algo support team.

## license Folder

If you would like to use Informacast on a device that hasn't been bundled with an Informacast license, you will need to purchase a license and put it into the license folder in the file manager.

## tones Folder

Custom audio files may be uploaded to play notifications. Audio files should be stored in the tones directory.

Existing files may be modified by downloading the original file, making the desired changes, then uploading the updated file with a different name. To download, right-click the tone and click Download.

Audio files must be in the following format:

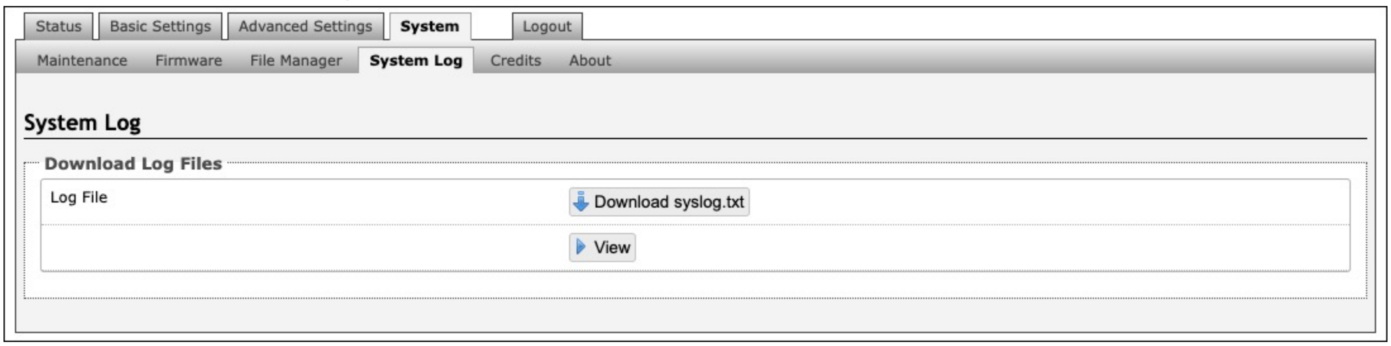
- WAV or MP3 format
- Smaller than 200 MB

File names must be limited to 32 characters, with no spaces.

For further instructions, reference the Custom Tone Conversion and Upload Guide.

## System Log

System log files are automatically created and can assist with troubleshooting if the device does not behave as expected.




---

# Log Out

Log out of the web interface.

---

# Specifications

View 8190 device technical specifications.

---

# FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operations of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at their own expense.

# Product Warnings

**Important Notice**

This product is powered by a certified limited power source (LPS), Power over Ethernet (PoE); through CAT5 or CAT6 connection wiring to an IEEE 802.3at PoE+ or 802.3af compliant network PoE switch. The product is intended for installation indoors. All wiring connections to the product must be in the same building. If the product is installed beyond the building perimeter or used in an inter-building application, the wiring connections must be protected against overvoltage/transient. Algo recommends that this product is installed by a qualified electrician.

If you are unable to understand the English language safety information then please contact Algo by email for assistance before attempting an installation support@algosolutions.com.

**Emergency Communication**

If used in an emergency communication application, the 8190 IP Speaker – Clock should be routinely tested. SNMP or ADMP supervision is recommended for assurance of proper operation. Contact Algo for other methods of operational assurance.

**Dry Location Only**

The 8190 IP Speaker – Clock is intended for dry indoor locations only. For outdoor locations Algo offers weatherproof speakers and strobe lights.

CAT5 or CAT6 connection wiring to an IEEE 802.3at PoE+ or 802.3af compliant network PoE switch must not leave the building perimeter without adequate lightning protection.

No wiring connected to the 8190 IP Speaker – Clock may leave the building perimeter without adequate lightning protection.